New Zealand Telecommunications Forum

Operations and Support Manual for Local and Mobile Number Portability in New Zealand

Version Number and Status:	**ENDORSED**
Version Date:	13 February 2025

This document forms part of the regulation for Number Portability and is enforceable through the IPMS Access Agreement.

Quick Start Guide

Overview

Customers are entitled to port under the LMNP Terms, under New Zealand law. The law requires that a Customer's numbers are portable. The LMNP Terms set out the expectations for the approval of port requests and activations of them.

Both the Gaining (GSP) and Losing (LSP) providers are expected to follow the rules. Those who resell the networks of others are also subject to those same rules.

The LSP response to a Port Request is expected within thirty minutes for a Mobile Port and eight hours for a Local Port. If the port is considered "complex" (i.e. many lines, pilots and steppers, centrex, ISDN) then the LSP has two days. Clearly anything beyond two days is not necessary, and therefore not acceptable.

The LSP is not permitted to reject a port request. The GSP is expected to approve or reject based on the result of the port request and the LSP response.

Porting is like Newton's Third Law – for every action there is an equal and opposite reaction. What that means is that for you to be able to port in, and enjoy the cooperation of the LSP, you must also cooperate with the GSP when a Customer ports out.

To enjoy the right to port numbers in, you must abide by the rules and expectations for porting out. Everyone is expected to respond to a port request within a reasonable time. Delayed responses will be seen as acceptance and the port will proceed.

Number Portability User Group (NPUG) meetings

Contact the TCF Forum Administrator to request to join the NPUG. Meetings are held once a fortnight and this is where major operational decisions are made. Config changes are tabled, and outages are often notified or mooted. A meeting typically takes less than half an hour. Attendance is not mandatory but is strongly encouraged. Agendas and minutes for NPUG meetings are available on the NPUG Shared Drive.

Operating Hours

For mobile, Operating Hours are 8am – 8pm, 7 days a week.

For local, 8am, 10am, and 12pm are the possible Ready for Service (RFS) times. Working Hours finish at 6pm.

You need to have automation and a way to escalate if you will not be on board and should talk to the LSP if you need to port outside of these hours.

Planned Outages

The preferred minimum notice period for a Planned Outage is two (2) Business Days. We try to have planned outages outside of Operating Hours, e.g. usually after 8pm. Notice must be sent to np.outages2017@tcf.org.nz and NPUserGroup@tcf.org.nz.

NPUG members will automatically be added to NPUserGroup@tcf.org.nz. Advise the Forum Administrator of any email addresses that should be added to np.outages2017@tcf.org.nz.

Unplanned outages

Unplanned outages will be notified through np.outages2017@tcf.org.nz and NPUserGroup@tcf.org.nz.

IPMS outages vs Carrier outages

The NP Coordinator will advise of IPMS outages, planned and unplanned. If a Carrier is having an outage and hasn't yet advised anyone then the NP Coordinator may choose to advise parties in the interests of portability. Questions about Carriers' outages are better referred to the NP Coordinator, rather than interrupt the Carrier who is having an outage. Please don't 'reply all' when responding to emails advising of an outage.

How to get hold of the NP Coordinator and escalation

If you are unsure of anything relating to porting, feel free to contact the NP Coordinator:

Rob Clarke
Rob.clarke@tcf.org.nz
021 956 501

Config documents

The vast majority of configuration information about IPMS is stored in the Config Worksheets. There is one per environment, and they include details on companies, Carriers, Service Providers, number blocks, system parameters and much more. These are stored on the NPUG Shared Drive.

Config changes

Changes in IPMS are made through config changes. Typically, they are formally notified at the NPUG meetings. We normally require two-weeks' notice for major SP changes and four-weeks' notice for major Carrier changes to PROD (changes in the TEST systems can be made much faster). Minor parameter changes could happen inside of 24 hours (where they don't impact everybody).

Other documents

There is a wide range of useful documents available on the NPUG Shared Drive that you may wish to refer to including training materials, process flow diagrams, API details, and much more. These include:

- The Beginner's Guide for IPMS users
- LMNP – New Entrant Guidelines
- Basic Getting Started API Calls for New Players
- LMNP – IPMS Porting Processes in Detail
- IPMS Process Guide

CONTENTS

1 EXPLANATORY STATEMENT

1.1 The purpose of this Operations and Support Manual for LMNP (the Manual) is for the support and assurance of Local and Mobile Number Portability in New Zealand. Its intent is to ensure that a consistent Customer experience (same processes, same Service Levels) is delivered by LMNP.

1.2 It is intended to provide detailed procedures for operational implementation and management of Porting Processes and multi-lateral issues that Service Providers and Carriers will need to implement to ensure and support the processes defined in the LMNP Terms and the Network Terms and information, such as Carrier contact details, that may vary.

1.3 Whilst this Manual may propose that some processes be subject to Bilateral Agreement, any such agreement shall not, in any way, result in a degradation of the Service Levels and Port Process expectations as laid out in either the LMNP Terms or this Manual.

1.4 The Manual applies to all parties to the Number Portability Determination in relation to either of the designated multi-network services, local telephone number portability service or cellular telephone number portability service.

1.5 This document should be read in conjunction with the following regulatory documentation produced by the Commerce Commission:

1.5.1 The Number Portability Determination Decision 554 – "Determination on the Multi Party Application for Determination of 'Local Telephone Number Portability Service' and 'cellular telephone number portability' for Designated Multi-Network Services" and Number Portability Clarification Decision 557 - Clarification of the Determination on the Multi-party Application for Determination of Local and Cellular Telephone Number Portability Designated Multi-Network Services";

1.5.2 Terms for Local and Mobile Number Portability (LMNP Terms);

1.5.3 Network Terms for Local and Mobile Number Portability (Network Terms).

A copy of these documents can be found on the TCF Website www.tcf.org.nz.

2 BACKGROUND

2.1 The Porting arrangements for Local Numbers and Mobile Numbers in New Zealand are provided by the Commerce Commission's Determination on the multi-party application for determination of 'local telephone number portability service' and 'cellular telephone number portability service' designated multi-network services, including any amendments and subsidiary determinations ("Number Portability Determination").

2.2 The Number Portability Determination includes the following:

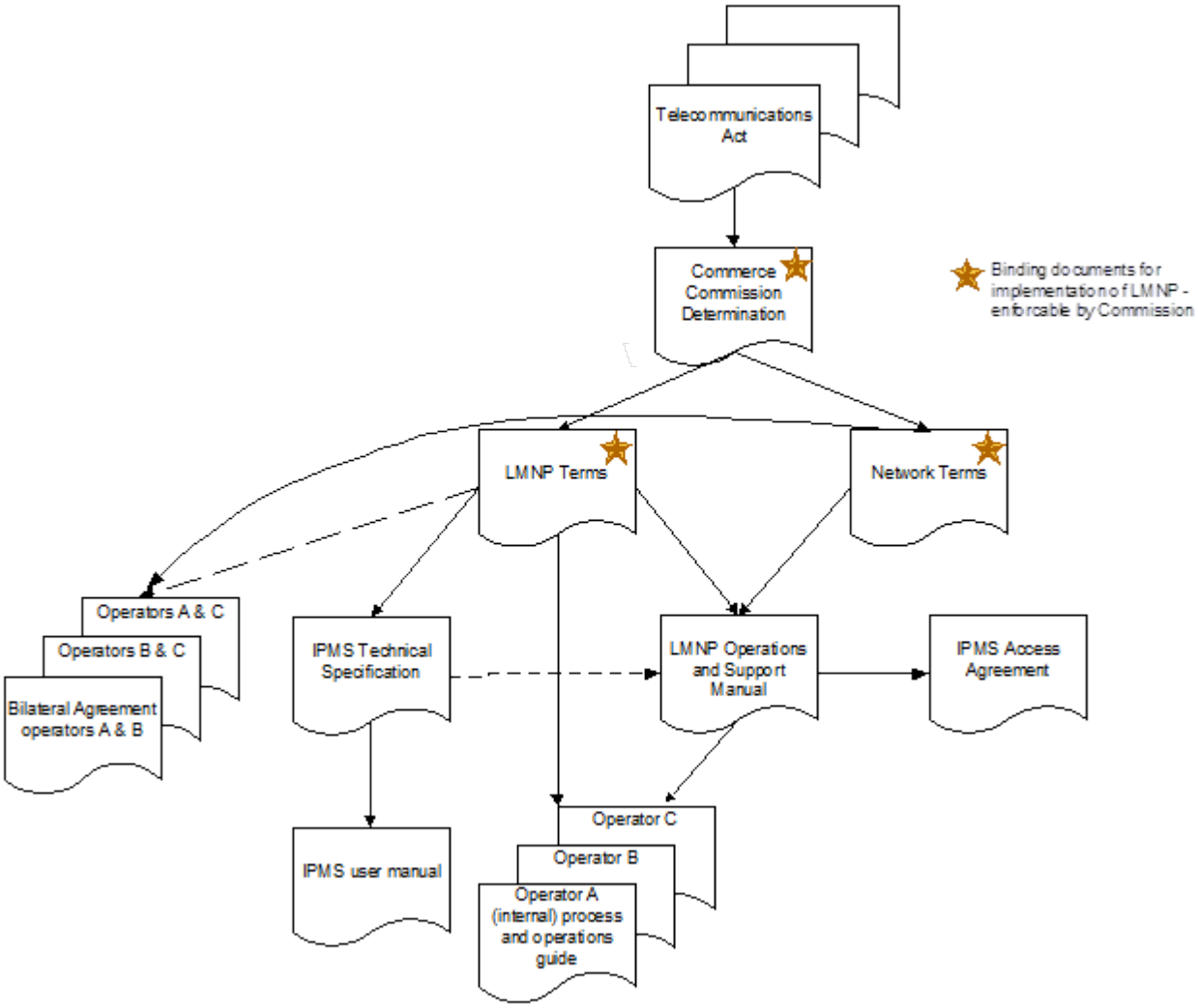
2.2.1 Terms for Local and Mobile Number Portability (LMNP Terms):

i The LMNP Terms detail the processes that enable Customers to Port their Local Numbers and Mobile Numbers and sets out the rights and obligations of parties to the LMNP Terms in a Local and Mobile Number Portability environment.

2.2.2 Network Terms for Local and Mobile Number Portability (Network Terms):

i The Network Terms is intended to guide participating Carriers in the development of their own Network solutions and specify the optional and mandatory requirements necessary between Networks for Local and Mobile Number Portability for Voice Services and Short Message Services.

2.3 Document Precedence



2.4 Changes in IPMS are reflected most rapidly in the Config Worksheet. It will eventually be reflected in this Manual, but this may take time.

2.5 Further Explanation

2.5.1 The IPMS Technical Specification document is used to specify the technical implementation of the IPMS. This needs to be read in conjunction with all subsequently published release notes.

2.5.2 Each Service Provider and Carrier is to produce their own internal manual of business processes and operational procedures. Their manuals are expected to be consistent with the LMNP Terms, the Network Terms and this Manual. These internal documents, however, have no official status in the context of LMNP.

3 CHANGE CONTROL PROCESS

3.1 Process for changing Operations Manual

Any changes to this Manual must be made in accordance with the TCF Rules and the IPMS Access Agreement.

3.2 Process for changing IPMS Parameters

The table below describes the process for requesting and implementing a parameter change in IPMS.

Step	Action	Organisation/Person Responsible
1	Parties to the Number Portability Determination and on-IPMS Resellers should discuss any change with the NP Coordinator who will raise the config change document and get approval before submission for system-wide changes. Changes within a party's own company don't require discussion or approval, just notice.	Party requesting the parameter change.

2	• Assign change number to change request.
	• Check the change, ensure it is consistent with the desired result and confirm the completed form contains all the required information for the proposed change.
	• Assess how much notice the change requires. Consideration of the impact on Carrier automation should be made.
	  ○ number range additions are done in accordance with PNCAs, donor changes and deletions are more complex.
	  ○ changes in TEST, DEV, or TRAIN can often be done with 24 hours' notice. If required, the restart will be done with minimal notice.
	  ○ changes in PROD normally require a minimum of 72 hours' notice. Restarts are normally done outside of Operating Hours.
	  ○ restarts for configuration changes may require a short outage outside of Operating Hours.
	• Notify NPUG.
	• Email the change request to the TCF Forum Administrator (along with a proposed timetable for all the environments) who will upload the change request
		NP Coordinator

	and the new Config Worksheet to the NPUG Shared Drive.	
3	Config changes are reported on at every NPUG meeting.	NP Coordinator
4	NPUG review: • It is preferred that the change is reviewed at an NPUG meeting but for urgent changes it may be distributed by email with at least one Business Day's notice before the restart. Any postponement should be done with a minimum of half a day's notice. • Agree to roll-out schedule.	NPUG
5	Review by the Parties to the Determination for more complex changes, such as a new Party joining: • All IPMS users are expected to review the impact of a config change on their own system and take appropriate action within the previously described notice periods.	Parties to the NP Determination
6	Manage roll-out of change: • Take note of any adverse reactions to config changes.	NP Coordinator

3.3 Standard or expedited process

The following IPMS parameter changes can follow the expedited process:

3.3.1 An existing Number range allocated by the NAD to the Party to the Determination that is already in use or about to be used that needs to be loaded into IPMS. (This situation may arise if a Carrier has omitted to load one of their existing Number ranges into IPMS).

3.3.2 Minor changes to the value of parameter fields in existing records for an existing System Parameter, Company, Service Provider or Carrier in IPMS TEST, IPMS TRAIN, or IPMS DEV environments.

3.3.3 Other changes in TEST, TRAIN, and DEV that are considered urgent and not too complex (there may be limits to how quickly the changes can be scripted) can be expedited if the NP Coordinator deems it to be practical.

3.3.4 Changes not requiring restarts of the environments impact others less and are more easily expedited.

3.3.5 Private configuration changes, such as parameter changes for a Carrier or Service Provider that impact only the party asking for the change, especially if it is to address something impacting portability in general.

3.4 If the NP Coordinator believes that a change could follow the expedited process and the change is not listed above, the NP Coordinator will expedite the change and advise the NPUG at the next meeting, or in an email with the new config document attached before the next meeting. The standard process would only occur where there is a change which impacts another Carrier.

In these cases, unanimous agreement is required by all members of the NPUG to proceed with the expedited process.

3.5 In cases where there is no impact on other Carriers and the NP Coordinator ascertains there is a benefit to portability in general, the change may be carried out and the NPUG notified afterwards. Once actioned, the configuration change would be uploaded to the NPUG Shared Drive and the NPUG advised at the fortnightly NPUG meeting.

4 DEFINITIONS AND INTERPRETATION

4.1 Terms defined in the Number Portability Determination and the IPMS Access Agreement have the same meaning in this Manual.

4.2 This section is intended to provide examples of the common expressions used for operational purposes.

Bilateral Agreement	Bilateral Agreements may be established between participants in LMNP and may be used to enhance the Service Level obligations of the Terms or to expedite the Porting Process. Care should be taken by parties entering into Bilateral Agreements, that the obligations outlined in the Terms are not compromised. A Bilateral Agreement check list is included in APPENDIX G.
BAU	Means business as usual.
Business Day	Means a day on which registered banks are open for normal banking business, excluding Sundays and nation-wide public holidays. Regional public holidays are considered to be Business Days.
Carrier	A Carrier is defined in the LMNP Terms. The Carriers and their allocated Hand Off Code (HOC) are available on the NPUG Shared Drive, in the Config Worksheet.
Config Worksheet	The latest version of this document is saved on the NPUG Shared Drive for each IPMS environment. This includes tabs on all major configuration elements, including Carriers, Service Providers, phone number ranges, service levels, system parameters.
Contractor	Means an onsite technician.
Customer	Unless specifically stated within the Manual – a person that has a bona fide retail billing relationship with a Service Provider.
IPMS	Means the Industry Portability Management System which is the software, hardware and other shared facilities used to give effect to the LMNP Terms set out in the Number Portability Determination.

IPMS Environments	The IPMS has five environments. PROD is the most important. We have two test environments: TEST and DEV. These are used for testing new builds of IPMS and for Carriers to test new versions of their own automation. TEST and DEV contain additional companies to facilitate testing. The NP Coordinator uses TRAIN for early beta testing and diagnosis. The PREPROD environment is meant to have production style data running the current version of IPMS software.
Local Port	Longer lead time and SLA time for activation. RFS time is only ever 8am, 10am or 12pm. Often multiple phone numbers per SOM. Frequently uses complex, which has even longer timeframes. Does not use 2FA for approval of port. The maximum number of phone numbers per SOM is 200.
Manual	Means the Operations and Support Manual for LMNP.
Mobile Port	Shorter SLA time for activation. Traditionally single number per SOM only, this might change. Uses 2FA for approval of port request. Never uses complex only ever simple. Requires either account number for postpay or SIM number for prepay.
Operating Hours	For mobile porting, ports can start between 8am and 8pm. So Operating Hours are 8am to 8.30pm.
NP Coordinator or TCF Coordinator	Means the party appointed by the by TCF to liaise with the System Administrator and is to be the primary contact point for any queries in respect of matters relating to the IPMS.
NPUG	Means the Number Portability User Group. Meetings of this group are held once a fortnight and are where major operational decisions are made.
NPUG Shared Drive	A central repository for documents relevant to NPUG members. Config documents, this Manual and supporting documents, NPUG meeting agendas and minutes can all be found here. Access to the NPUG Shared Drive can be requested from the TCF Forum Administrator.
Service Provider	Service Provider is defined in the LMNP Terms. The list of Service Providers bound by the Number Portability Determination as Access Seekers or Access Providers is available on www.tcf.org.nz.
System Administrator	Means the party appointed by the TCF from time to time to maintain and operate the IPMS.
TCF Forum Administrator	Means the party appointed by the TCF to provide all analytical, secretariat, communications, accounting services and website support to the TCF.

Terms	Means the LMNP Terms and Network Terms (as the context requires).
Working Hours	Working Hours are defined as being between 8am and 6pm on Business Days (as defined above). These are often used for SLA monitoring. Note that Mobile porting operates between 8am and 8pm, so planned outages need to happen beyond that timeframe.

5 OVERVIEW OF THE IPMS ENVIRONMENTS

5.1 The IPMS has five environments visible and accessible by IPMS users:

5.1.1 **IPMS TEST** – The primary purpose of this environment is to load new builds of IPMS so that they can be acceptance tested by IPMS users before being deployed into PROD. TEST includes additional companies (Dummy and the FBN Companies) to facilitate testing, has number ranges configured for minimal Network Updates, and the data bears little resemblance to PROD.

5.1.2 **IPMS DEV** – this is used very much like IPMS TEST. New builds are deployed to TEST and DEV at the same time.

5.1.3 **IPMS PREPROD** – This has a relatively recent copy of PROD data and runs on a separate Virtual Machine (is configured identically to PROD). It is used for final testing, particularly load oriented testing, before deployment of new software versions to PROD. It is also used for testing SQL scripts that may not be able to be run in IPMS TEST. Carriers can run testing of their own automation against PREPROD knowing it is running the same IPMS version as PROD (usually, not always, there are brief times when they are not during the transition to a new build).

5.1.4 **IPMS TRAIN** - runs as an instance on the same server as TEST and DEV, the TRAIN Database also runs on the shared test database server. The database is a copy of PROD, not renewed very often, but has close to PROD number ranges, and no Dummy or FBN Companies. Beta testing of new builds is done here.

5.1.5 **IPMS PROD** – The live number portability environment.

5.2 References to IPMS in this Manual refer only to the PROD environment, though the processes described can be recreated in the test environments for the purposes of testing, without impacting real world users and other parties.

5.3 Development by the Application Support team is tested on another environment that is inaccessible to all but that team.

5.4 Both TEST and DEV contain additional fictional parties (not found in PROD) to make testing easier. The original LMNP parties have FBN (Fly By Night) versions of their own companies (i.e. Spark and FBN Spark). Parties that were loaded into IPMS subsequently all use the Dummy Company, and are given userids for this company. These fictional parties can be used to act as the other party (e.g. GSP or LSP etc) for testing work because all porting activity requires responses from at least one other party for activities to be completed.

5.5 Number ranges in TEST and DEV can be very different to those in PROD. In particular, because there is no real-world call routing occurring in these two environments, there are a number of ranges that have a reduced set of networks that receive network updates. This facilitates faster testing. A list of these Queueing By Number Range (QBNR) numbers can be found in the relevant Config Worksheet.

6 SECURITY OF IPMS

6.1 Given the critical nature of the IPMS system, the TCF recognises the importance in having oversight of who uses the system and ensuring that Parties to the Determination and other authorised entities that use IPMS adhere to good security practices.

6.2 Access to IPMS is only granted to users with the appropriate security credentials. All users, as well as all IPMS related activity, must adhere to the TCF's approved Security Policies for IPMS, as set out in APPENDIX F.

6.3 From time to time the capability for monitoring security will change and processes will be adapted to reflect that.

7 IPMS PARAMETERS

7.1 There are parameters in IPMS that can be modified as required. Sometimes they may be changed rapidly or temporarily in the interests of allowing portability to function. The key ones are recorded here as a guide and to add visibility to them.

IPMS Parameter Name	Current Value	Description and function
maxAPCsPerPort	10	This limits how many APCs may occur on a single SOM, more than three or four is considered impolite. Ten should almost never be achieved.
expiredBusinessDays	5	If an expiring SOM is not APC'd, then six (5+1) business days after RFS it becomes expired. This is end of life for that SOM, a new SOM can be raised with those numbers.
expiringBusinessDays	1	When an approved port is not activated at RFS, it becomes expiring after this many business days.
localNumberPortWindows	08, 10, 12	These are the times that are legal local SOM RFS times. See Service Level table for the RFS Window for each Port Type.
maxNetworkUpdatesReturned	150	This is to control how much information is returned in getNetworkUpdates to prevent Carrier automation from being swamped in a backlog situation.

IPMS Parameter Name	Current Value	Description and function
maxPhoneNumbersPerPort	200	This is the largest SOM currently allowed.
maxPortResubmissions	10	If you need to submit the same port request more than ten times, you really need to check your information.
workingDayEndTime	18:00	Working hours end at 18:00
workingDayStartTime	08:00	Working hours start at 08:00

7.2 The full list of parameters is available in the System Parameter tab of the IPMS PROD configuration worksheet, available on the web site.

8 CODE OF CONDUCT

8.1 Good Faith

8.1.1 All parties shall act co-operatively and in good faith to facilitate Porting Processes.

8.1.2 All parties must act in a non-discriminatory manner and must facilitate Porting by acting in compliance with principles and processes that are consistent with section 18 of the Telecommunications Act.

8.1.3 Each party subject to the LMNP Terms must comply with the Service Levels. If a party fails to meet the Service Levels, the provisions set out in clauses 127 to 142 of the LMNP Terms will apply.

8.2 Porting is all about give and take. In any given port, the GSP is highly motivated to make it succeed, but the LSP is less so.

8.2.1 The GSP needs to ensure that the Port Request they submit is complete and credible, and as accurate as possible with the available information. The LSP is not expected to do all the work.

8.2.2 The GSP may on occasion need assistance from the LSP, due to issues with numbers in the Port Request, or timing constraints that may require concessions from the LSP. However, this is a two-way street, and you cannot expect special attention for every inbound port unless you are ready to cooperate as the LSP.

9 RESELLERS

9.1 A Customer should be able to experience the same porting process regardless of whether their Service Provider is a user of IPMS directly or is a Reseller.

9.2 The fact that a Customer is being billed through a Non-IPMS Based Reseller who has failed to respond to a porting step within the timeframes provided under the relevant Service Level is not sufficient grounds to reject or delay a porting step. A party's obligations to adhere to the Service Levels are not abrogated by the involvement of a third-party Reseller.

9.3 The Wholesaling Service Provider is responsible for ensuring, to the best of its abilities, that any of its Resellers do not delay the approval of a Port Request. They are not entitled to refuse a Port Request (which isn't possible). This obligation includes ensuring that approval for porting steps is granted in a timely manner so that the Service Provider or Carrier can comply with its Service Level obligations under the LMNP Terms. Each Service Provider and Carrier shall include a clause in its contract with its Resellers that binds the Reseller to support the Service Provider or Carrier in their obligation to support Number Portability in accordance with the LMNP Terms and this Manual. These terms may include an ability for the Service Provider or Carrier to approve porting steps on behalf of the Reseller if the Reseller's delay is at risk of forcing the Service Provider or Carrier to breach a Service Level under the LMNP Terms.

9.4 The off-IPMS Reseller is expected to comply with the requirements of the Terms in the same timeframe as other port requests. They are not allowed to approach the Customer as the result of a port request. All they are required to do is confirm that the named Customer is being billed for the numbers in the port and to supply the account number used for those phone numbers. The Reseller has no right to refuse a port request. The absence of a response within the appropriate timeframe will be considered to be confirmation that the supplied details are correct.

9.5 Below is some text that can be used in third-party validation requests, outlining Resellers' obligations:

9.5.1 Customers are entitled to port under the LMNP Terms, under New Zealand law.

9.5.2 A Customer is entitled port their number at any time by providing their existing retail provider details to a new provider, without prior notification to their current provider. However, the porting of their numbers does not end any existing obligations the Customer may have to their existing provider.

9.5.3 Both the gaining and losing providers are required to follow the rules outlined in the Terms, and those who resell the network of others are subject to those same rules.

9.5.4 The purpose of the third-party validation request is for the Reseller to confirm that the supplied account detail is correct. If the Customer account detail supplied is correct, then the LSP response should not prevent approval.

9.5.5 The LSP response to a Port Request is expected within thirty minutes for a mobile port and eight hours for a local port. If the port is considered "complex" (i.e., many lines, pilots and steppers, centrex, ISDN) then the LSP has two Business Days. The absence of a response in within the required timeframe will be considered to be confirmation that the supplied details are correct.

9.5.6 All ports require cooperation between the GSP and LSP, the GC and the LC. Being helpful, competent, and responsive as the LSP is necessary if you wish others to extend you the same courtesy when you are the GSP.

10 PORTING FOIBLES

10.1 The NPUG has identified the following items of particular importance that cause confusion or can create delays in the porting process if they are not well known and understood. Though

IPMS users should be aware of all aspects of Number Portability covered in this Manual, the following items are highlighted as having particular importance.

10.2 Only active numbers may port

10.2.1 Disconnected numbers cannot normally be ported, they have no account number associated with them. You need to talk to the donor to arrange activation if a disconnected number is required.

10.3 Faxability

10.3.1 Customers are often unaware that they have a legacy faxability number but failing to include a faxability number in a port request often results in a failure to achieve approval. Faxability numbers can be discovered using wireline.

10.4 Not required (Not Req)

10.4.1 Do NOT tick this box unless you do not want the number to be ported in this SOM. A Not Required number will remain with the LSP.

10.4.2 Some LSPs, specifically Spark and Voyager, will disconnect Not Required lines.

10.5 LSP Override

10.5.1 You can check the LSP for a number by doing a number enquiry. Sometimes, IPMS will display a different LSP than that provided by the Customer. This will always happen with third-party Resellers. If IPMS has the incorrect LSP listed, you can:

10.5.2 Check with the Service Provider that IPMS lists as the LSP first. This is a courtesy, but it is also efficient at identifying whether you can proceed submitting the port to them for them to action on behalf of a Reseller, or whether there are any potential issues that might ultimately result in a failed port.

10.5.3 If the GSP is certain that the details they have been given are correct, or if they are listed as the existing Service Provider, they can put through a port request with the actual LSP and where they select the correct GC. IPMS will automatically reject this port but once that happens, the GSP can check the “LSP Override” box and resubmit it. This is the only legitimate time you can use LSP override.

10.6 Emergency Returns

10.6.1 The separate Emergency Return process has been retired. It is best to contact the original Service Provider and agree to do a normal Port Request, including an associated APC to set the RFS date immediately.

11 PORTING PROCESS

11.1 The Porting Process means the process described in clauses 146 to 318 of the LMNP Terms.

11.2 A detailed description of the Porting Process is covered in a separate document, LMNP – IPMS Porting Processes in Detail, available on the NPUG Shared Drive.

12 BULK PORTS, MIGRATIONS, AND SPECIAL PROJECTS

12.1 Any porting project involving more than a thousand numbers in a short period or any sustained volume over 300 numbers per day should be logged with the NP Coordinator. These need to be managed carefully to ensure it doesn't swamp the Losing Carrier or diminish service for others. Notification should include an indication of quantity, start date, and desired completion date. Then a timetable will be agreed based on other expected volumes. Progress should be updated during the project.

12.2 Where a bulk change involves a change in Service Provider only with no change in Carrier, we have a tool to perform this change at around 20,000 numbers per batch, talk to the NP Coordinator about timing.

12.3 A special project was a method for handling a large volume of ports outside the standard porting process.

12.3.1 It required Carriers who process Network Updates to import the changes outside IPMS, and many Carriers have not ever used it. It is rarely used now because day-to-day porting processes can handle considerable volume. Local ports can be put through 200 numbers per SOM. This will soon be possible in Mobile when all Carriers are ready.

12.3.2 Now that there are 14 Carriers consuming network updates the use of a migration data file is logistically impractical. If you feel that there is a need for such a project talk to the NP Coordinator.

12.3.3 More details on special projects and bulk migration can be found in APPENDIX B

13 SERVICE LEVEL EXPECTATIONS AND OPERATING HOURS

13.1 Working Hours and Operating Hours are slightly different, as defined in section 4.

13.2 These times are correct at the time of printing but are subject to change (when agreed by NPUG) and the most authoritative source of the current state is in the IPMS PROD Config Worksheet.

13.3 Formally measured SLAs focus on Port Activation. These are Working Hours only.

Port Activation

Network	Port Type	GSP	LC	Total
Local	Complex	4 hours	4 hours	8 hours
Local	Simple	4 hours	1 hour	5 hours
Mobile	Complex	N/A	N/A	N/A
Mobile	Simple	30 minutes	10 minutes	40 minutes

13.4 Network updates are expected to be completed within 60 minutes.

13.5 We can alert you when LC done occurs and activation is ready for completion if you don't have these processes automated.

13.6 Other actions in IPMS are not formally measured. They are (Working Hours):

Network	Port type	Minimum notice	LSP response	APC acceptance
Local	Complex	40 hours	2 Business Days	4 hours
Local	Simple	16 hours	8 hours	2 hours
Mobile	Complex	N/A	N/A	N/A
Mobile	Simple	0 minutes (2FA really needs 4 hours)	30 minutes	2 hours

13.7 If you have trouble responding to APCs in time, we can send you reminder emails about required LSP responses, APC acceptance. Date-change only APCs can be automatically accepted if desired.

13.8 For further explanation of the Service Levels, refer to Table 2 of the LMNP Terms.

14 AGENCY AND SPECIAL SERVICES REQUIREMENTS (EMERGENCY SERVICES)

14.1 There are organisations that have a genuine need to access information about ported numbers. This may be in the form of single number enquiry or downloading the full number register. Organisations need to liaise with the TCF to arrange the service and sign an agreement.

15 CUSTOMER FAULT HANDLING AND TESTING PROCEDURES

15.1 If you identify a fault with a recently ported number and everything in your network checks out it is worthwhile to check with the LSP first and then, if need be, get the NP Coordinator to check for issues in IPMS or with other Carriers.

15.2 For further details see APPENDIX C.

16 PORTING ASSISTANCE AND COMMUNICATION

16.1 When you are having a problem with a port and you seek help, be aware of the following:

- The NP Coordinator might be the best first person to contact.
- It is fine to copy the NP Coordinator on your email if it is to another Carrier.
- Make sure you include all the important information in your request (e.g. SOM number, phone numbers, specifics about the problem).

16.2 For more detail on contact procedures, refer to APPENDIX A.

17 IPMS FAULT MANAGEMENT

17.1 Contact the NP Coordinator immediately in the case of any suspected IPMS issue or fault. In an outage situation, the phone is quicker than an email.

Rob Clarke
Rob.clarke@tcf.org.nz
021 956 501

17.2 APPENDIX H details actions that may be taken for various outage or performance issues.

18 CAPACITY FORECASTING PROCEDURES

18.1 We no longer need formal volume forecasting as IPMS is able to handle considerable variation in activity levels, as are the Carriers.

18.2 If a planned project involves more than 300 numbers a day, the NP Coordinator should be advised, as per section on Bulk Migration. It may need to be discussed at an NPUG meeting.

19 NEW PARTICIPANTS PROCEDURES

19.1 A new Carrier who joins the NAD is required to be part of LMNP when they are allocated a HOC and/or number blocks.

19.2 The separate document LMNP – New Participants Procedures describes how new parties who wish to participate in Number Portability need to work with the TCF and the parties to the Number Portability Determination to provide a satisfactory Porting experience for Customers.

19.3 A Service Provider who solely uses a third-party Carrier may join LMNP as a Reseller.

19.4 Some Service Providers may choose to operate solely within the company of their chosen Carrier.

19.5 Existing Parties to the Number Portability Determination must review internal Porting processes and systems to incorporate the new Service Provider.

19.6 The minimum notice for changes in IPMS PROD are:

- New SP: 2 weeks
- New Carrier: 4 weeks (testing date and ready date often specified in PNCA)
- New Company: 4 weeks (if it includes a new Carrier, 2 weeks if just a new Service Provider)
- Minor changes to any of the above: may be 2 weeks or less (particularly when no action required by other Carriers).

20 ENFORCEMENT AGENCY PROCEDURES

20.1 Every month the Enforcement Agent will send notices of Breach to those who have not reached service levels. See APPENDIX E for details.

21 SYSTEM AND NETWORK OUTAGES

21.1 Planned Outages

The preferred minimum notice period for a Planned Outage is 2 Business Days. We try to have planned outages outside of Operating Hours, e.g. usually after 8pm. Notice must be sent to np.outages2017@tcf.org.nz and NPUserGroup@tcf.org.nz.

21.2 Unplanned outages

Unplanned outages will be notified through np.outages2017@tcf.org.nz and NPUserGroup@tcf.org.nz.

21.3 IPMS outages vs Carrier outages

NP Coordinator will advise of IPMS outages, planned and unplanned. If a Carrier is having an outage and hasn't yet advised anyone then the NP Coordinator may choose to advise parties in the interests of portability. Questions about Carriers' outages are better referred to the NP Coordinator, rather than interrupt the Carrier who is having an outage. Please don't 'reply all' when responding to emails advising of an outage.

21.4 Further details are included in the Network Terms.

22 BLACKOUTS

22.1 Blackout functionality was introduced to IPMS in build 3.0.3 in mid-2017.

22.2 A blackout merely prevents port requests from having an RFS date during an expected outage and stops any APC from being moved to the blackout period. IPMS continues to operate normally.

22.3 During the blackout ports can still be scheduled for RFS dates beyond the blackout window. In-flight activations may also be advanced, and network updates can be completed, however if the LC or a key Network Update consumer is the reason for the blackout, then service will be severely degraded.

22.4 Sometimes a blackout will be used for a planned IPMS outage, in which case normal operation will not be possible, but the blackout prevents the outage from impacting port activations.

22.5 With the arrival of 2FA, we use daily blackouts from 8pm to 7:59am to prevent Mobile Ports at a time where SMS approval is inappropriate.

22.6 If the blackout is for a Carrier, they advise the NP Coordinator with brief details (Start, end date and time, brief reason for it).

22.7 Typically, the blackout is loaded to start 30 minutes before the outage commences to allow time for in-flight ports to complete and prevent SOMs starting immediately before the blackout.

22.8 The NP Coordinator will load the blackout into IPMS, update the IPMS home page, and check for any existing SOMs that have an RFS in the blackout period. All Carriers with SOMs in that period will be advised by email with a list of SOMs and with advice to APC them out of the danger zone.

22.9 A planned Carrier outage doesn't always require a blackout, but if a key Carrier (particularly those processing network updates) is unable to process NUs for any length of time, then port activations should be prevented during that period.

22.10 Blackouts are also used for new IPMS build installs, DR shifts, Oracle patches, and other events occurring centrally.

22.11 We use blackouts at just 8am, 10am and 12pm on public holidays to stop local porting on days like Christmas Day.

22.12 Sometimes an overnight blackout may be shortened to allow a Carrier to perform Production testing without impacting LMNP in general.

23 DISASTER RECOVERY

23.1 DR synchronises every two minutes from IPMS PROD, therefore In a DR situation, parties will lose no more than two minutes of transactions.

23.2 The DR process is tested at least annually by shifting IPMS PROD to the DR Site for a week and then it is returned to the Primary Site. This happens outside Working Hours.

23.3 During Working Hours, IPMS logs an average of 8.9 transactions per minute (these are loggable, successful transactions, so it excludes read-only transactions and failed calls). This means that there should be no more than 20 transactions lost in a forced DR shift.

23.4 As per clause 357 of the Terms, IPMS is considered the primary source of information and if Carriers disagree with IPMS, then it is IPMS that takes precedence.

23.5 All Carriers and Service Providers need to check their own records of the state of outstanding SOMs and the numbers therein against IPMS PROD once it comes up at the DR Site. They should focus on in-flight activations and recently closed ports and then move to other outstanding but less urgent SOMs.

23.6 Carriers and Service Providers should develop their own processes for reconciling their systems against IPMS to ensure they recover from a DR shift as quickly as possible.

23.7 The best approach is to simply repeat those missing steps, possibly using the IPMS GUI if the Carrier automation can't readily re-process transactions that have already occurred.

24 UNAUTHORISED PORTS

24.1 If a port is deemed to be unauthorised, the LSP of the unauthorised port needs to liaise with the GSP to expedite a reversing port.

24.2 See clauses 71 and 72 of the LMNP Terms for details.

25 CALL READDRESS

25.1 Call Readdress is an old pre number portability method for a number to change Carriers. Very few numbers remain in this setup. See APPENDIX D for details.

26 2FA SMS FOR MOBILE PORTING

26.1 Mobile Ports requested through the GSP's Customer portal should always use 2FA.

26.2 If a Customer is at a provider's store and they cannot respond to the 2FA SMS and it is certain they have the right person then 2FA can be overridden. Call centre staff should not have the authority to skip 2FA.

26.3 There are other situations where 2FA is not required, such as where the customer has been with the new SP for some time, and used that phone number as their contact number, or with multiple numbers in the case of Corporate or Business accounts.

26.4 Where a GSP does not use 2FA, the LSP might enquire as to why and what evidence they have, to suggest that 2FA was not required.

APPENDIX A. PORTING CONTACT AND ESCALATION POINTS

This section provides guidelines on how and when to contact other parties in regards to Porting.

Maintenance of contacts – all parties need to ensure that their contact details in the NP list are correct and up to date. These contact addresses should not be auto-responding bots.

When using the np.outages2017@tcf.org.nz and NPUserGroup@tcf.org.nz addresses, it is preferred to BCC them to avoid a spam storm of responders.

Communication

Communication should include:

Initiator of the contact	• First level contact (refer to contact list)
Contact at other provider	• First level contact (refer to contact list)
Method of contact	• Email shall be the primary method of contact between parties • Phone calls should be used where Service Levels are short (e.g. simple mobile), or the issue is critical. • Phone contact should be followed up by the initiator with an email to confirm the issue discussed and the agreed outcome.
Minimum information to supply (requestor)	• SOM • Phone number • Reason for contact and action requested • Priority of request
Optional information to share	• Copy of Customer Authorisation form • Customer name, address • Further information as appropriate
Response time	• Resolution during initial contact where possible. • Otherwise response within 2 hours by the contacted party to provide an update on the request, and an estimated time for resolution where applicable. • Different response times may apply outside of Working Hours

Escalation points

Escalation points for Porting will be maintained on the NPUG Shared Drive.

APPENDIX B. SPECIAL PROJECTS

This is very rarely used now because day-to-day porting can handle larger volumes of ports (300 per day). It is also more complicated because there are now 14 Carriers processing network updates and many have never used the special project methodology. This needs to be discussed with the NP Coordinator before a special project can proceed.

In addition to the four types of Ports listed above, there may be a need to update IPMS and / or third-party Carriers outside the provisions of the standard Simple and Complex porting process. This update will require the IPMS manager to generate a ported number change file which is to comply with the structure shown in the table below.

- A Special Project necessitating update of IPMS would involve a direct load of Numbers or changes to the IPMS database, bypassing the Port processes (i.e. the messages and SLA's) as they exist for Simple and Complex Port types.
- A Special Project may involve any combination of change of Service Provider, change of Carrier and change of Donor Carrier or any instance where IPMS needs to 'know about' changes in order to either maintain network call handling integrity, or allow future Ports on the affected Numbers.[1]
- This type of update must not be used for Customer initiated Ports for fewer than 5,000 numbers.
- Special projects should be clearly defined upfront by means of a terms of reference. This document should clearly outline and include the scope of the project, impacted stakeholders, roles and responsibilities and a schedule of events. The scope should be agreed prior to the start of the project. It will be the role of the NP Coordinator to ensure the Terms of Reference template is completed and to manage the project from start to end.

1 Per line set-up costs may be applicable

Special Projects Upload Structure		
Header record		
Field name	**Data Type**	**Description**
Company Name	One String – VarChar(50)	Company name as defined in IPMS database, e.g. ”One NZ Ltd”
File Date and Time	DateTime – DDMMMYYYY HH:MM:SS	Date and time when file was created, e.g. 31NOV2005 23:59:59
Detail record		
Field name	**Data Type**	**Description**
Number	VarChar(11)	String of up to 11 numeric digits, including area code or prefix with leading zero, e.g. 0271234567 for Mobile, or 097654321 for Local Numbers
Carrier Name	Integer	ID of one of the Carriers defined in IPMS database, e.g. 11407
Service Provider Name	One String – VarChar(50)	Name of one of the Service Providers defined in IPMS database, e.g. “One NZ”

All LMNP parties have a responsibility to fully disclose to the NPUG, any planned work on internal systems which interface to IPMS or as may enable third parties, such as Resellers, to provide porting capabilities.

The NPUG has a responsibility to ensure a consistent Customer experience (ref clause 1.1 of this Manual). To ensure this consistency, they may implement governance in a manner similar to that of a Special Project.

Third party updates may be implemented:

- Updates shall be implemented through the Special Project migration file.

Obligations

As the SLA’s defined in the LMNP Terms do not apply to the Special Project event, the following obligations shall apply:

- The initiating party must provide a minimum notice period of 20 Business Days prior to the generation of the Terms of Reference notification to all parties to the Number Portability Determination.
- Special Project timelines are to be developed with all parties impacted by the Special Project, working in good faith on an individual project basis. This notwithstanding, any party unable to fulfil the requirements of the Terms of Reference within 40 Business Days of its formal notification shall formally notify the NP Coordinator of this.

APPENDIX C. CUSTOMER FAULT HANDLING AND TESTING PROCEDURES

1 Objectives

1.1 To identify how Carriers / Service Providers will act in the event of a Ported Number fault and provide processes and requirements for the management / resolution of Network faults involving Number Portability.

2 Guidelines

2.1 Each Carrier will progress their own fault handling within their own Network. Each Service Provider is responsible for their Customer base and as such will have control of any service fault reports.

2.2 The specific inter-Carrier process for Number Portability fault handling and resolution are to be developed by Carriers as amendments to existing Bilateral Agreements regarding fault handling.

2.3 If the location of the fault is determined to be in the Host Carrier network then responsibility for management and repair of the fault shall be with the Host Carrier.

2.4 If the location of the fault is determined to be in the Donor Carrier network then responsibility for management and repair of the fault shall pass to the Donor Carrier.

2.5 The party responsible for the fault shall repair the fault within the clearance times given in the three tables below unless the fault has no impact on services provided to the other party under this agreement. If temporary repairs are made, the other party shall be informed and agree to the estimate of the timescale to full repair and the expected impact on the service.

2.6 The party responsible for fault repair shall inform the other party using an agreed communication format as soon as the fault is resolved.

Standard Testing / Fault Analysis

2.7 Before reporting a fault to another Carrier, each Carrier must ensure that the:

- Port Activation time for Porting has expired
- Customer Equipment is correctly terminated
- Dial tone or an outgoing call capability is available on the Gaining Carrier service
- Test calls from within the Gaining Carrier telecommunications Network are successful; and
- Test calls from other Carrier Telecommunications Network are unsuccessful.

2.8 Each Carrier whilst diagnosing a fault must use sufficient analysis to identify which Carrier Telecommunications Network may be causing the fault and then direct the fault report to the now identified Carrier in the first instance.

Additional Testing / Analysis for Complex Ports

2.9 In the case of a fault with a Complex Port, the Gaining Carrier must conduct the Standard Tests however the Gaining Carrier does not need to test all Numbers if there are more than 10 Numbers associated with a service which are in a sequential Number range.

2.10 In the case where there are more than 10 sequential numbers, the Gaining Carrier must apply Standard Tests for the following Numbers:

- the first Number in the range
- the last Number in the range
- a selection of Numbers in the range representing an even spread of the range, such that five Numbers or 3% of the range (whichever is greater) are tested, ensuring that testing includes a minimum of three Numbers in each 100 Number Block.

Guide to LMNP Fault Management Timetable

2.11 Further evaluation of the impact on existing BAU fault management processes. Each needs to be checked against existing Bilateral Agreements.

2.12 This section is intended to provide guidelines for inter-company fault resolution Service Level Agreements.

2.13 Fault priority levels are defined as follows:

- Upon initial contact between the parties involved in the fault process, the party receiving the fault will set the initial priority, and confirm status and priority to the other parties, observing response times as specified in the Service Level table in this section.

Priority	Fault
1	Critical impact, e.g. Complete outage of a service or loss or severe degradation of inter-Carrier exchange capability.
2	One or more Customers are experiencing partial loss of service to access either inbound or outbound calling (not both) impacted
3	All other faults

2.14 Either party may request reclassification of a priority 2 fault to priority 1- this reclassification must be agreed between the parties.

2.15 The quality of service parameters appropriate to the fault management procedure is specified below.

Period Title	Value
Response Time	Time between an intercompany fault report and the first response from the Service Provider/Carrier that clearly indicates expected resolution time, progress information and fault diagnoses.
Resolution Time	Time between fault report and fault resolution.
First Escalation Time	Time between the Fault initially being reported and the relevant escalation contact point first being informed.
Second Escalation Time	Time between an intercompany fault being reported to the first escalation point and the relevant second escalation point contact first being informed.

Note: a fault may be escalated if the agreed resolution time is not met, or updates are not received within the agreed timeframes.

2.16 The service parameter values for all services are specified below:

- The Service Levels in the table below relate to Business Days and Working Hours. After hours fault Service Level timeframes to be checked through Bilateral Agreement process.

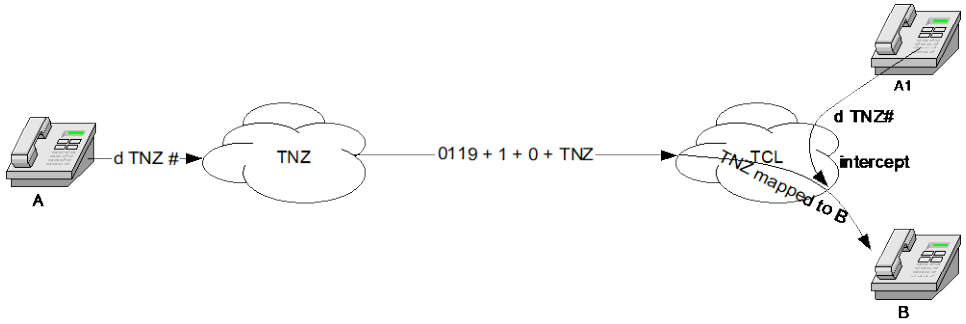
	Priority 1	**Priority 2**	**Priority 3**
Response Time	< 30 min	< 120 min	< 2 days
Resolution Time	4 hours	8 hours	3 days
First Escalation Time	2 hours	8 hours	3 days
Second Escalation Time	4 hours	2 days	5 days

APPENDIX D. CALL READDRESS

Call Readdress is a network capability between two working numbers, each on a different Service Provider's network that allows one to be diverted to another. Call Readdress is no longer available for new connections to Customers and therefore over time the numbers should diminish with the Porting alternative. There are two types of Call Readdress that exist: Full Call Readdress and Partial Call Readdress.

1 Full Call Readdress

1.1 Full Call Readdress, is effectively an alternative name for a donor re route scenario. Donor re route is a valid call forwarding service whereby end-users call the Customer by dialling the listed number which is routed to the donor Carrier. The donor Carrier then Call Forwards to the recipient network with Called Party Number equal to HOC + Call Readdressed Number as shown in the diagram below.



Scenario 1

- Spark Customer (A) dials Spark number that is diverted to VF
- Call forwarded to VF as HOC 0119+1+0+Spark Number
- VF Terminates Call to (B) – Spark Number configured on VF switch to map to (B)

Scenario 2

- VF Customer (A1) dials Spark diverted number
- VF intercepts call and terminates to (B) via Spark # mapped on switch

1.2 When a Full Call Readdress Customer originates a call, their CLI is set to the Call Forwarded Number.

1.3 Whilst this was a pre-Number Portability mechanism, Full Call Readdress required all calls not ported to the originating Carrier[2] to be sent to the donor Carrier. As this scenario maps simply to the originating Carrier lookup scenario, with its inherent advantages, Full Call Readdressed numbers have been migrated over to the LMNP Port process.

2 Partial Call Readdress

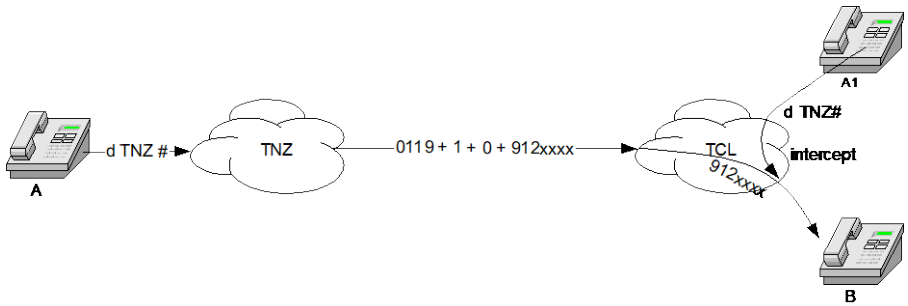
2.1 For Partial Call Re-address, the call forwarded Customer is assigned two numbers:

- one number is their original number from the donor network (the "Call Forwarded Number");
- the second number is a number from the call forwarded or recipient Carrier network (the "Recipient Network Number").

2.2 End Users can call the Partial Call Readdress Customer by dialling either the Call Forwarded Number or the Recipient Network Number.

2.3 If the End User dials the Recipient Network Number, the call is routed directly to the recipient network bypassing the donor switch.

2.4 The diagram below illustrates two call scenarios when an End User dials the Call Forwarded Number of a Partial Call Readdress Customer:



Scenario 1

- Spark Customer (A) dials Spark number ported to VF
- Call forwarded to VF as HOC 0119+1+0+VF#
- VF terminates call to (B) VF# e.g. 912 xxxx

[2] Interceptions are in place to trap calls to numbers ported to the Carrier originating the call

Scenario 2

- VF Customer (A1) dials Spark number ported to VF
- VF intercepts call and terminates to VF 912xxxx (B)

3 Call Readdress Procedures

3.1 The Gaining Service Provider (GSP) is to provide all Customer details including the number to be ported and the Partial Call Readdress number associated to it.

3.2 The LMNP Terms state it is the responsibility of the GSP to prepare the Port Request. The Port Request must include the data required as per Appendix 1, Table 1 of the LMNP Terms. Subject to clause 37 of the LMNP Terms, the Losing Service Provider (LSP) is not obliged to advise the GSP of additional Numbers beyond those included in the Port Request (see clause 75.3 of the LMNP Terms).

3.3 However, when the LSP checks the Port Request, subject to clause 171 of the LMNP Terms, the LSP enters its understanding of the details if they differ from the information presented by the IPMS and this can include the addition or removal of Numbers for a Multiple Number Port (see clause 170 of the LMNP Terms).

4 GSP Rules for Partial Call Readdress

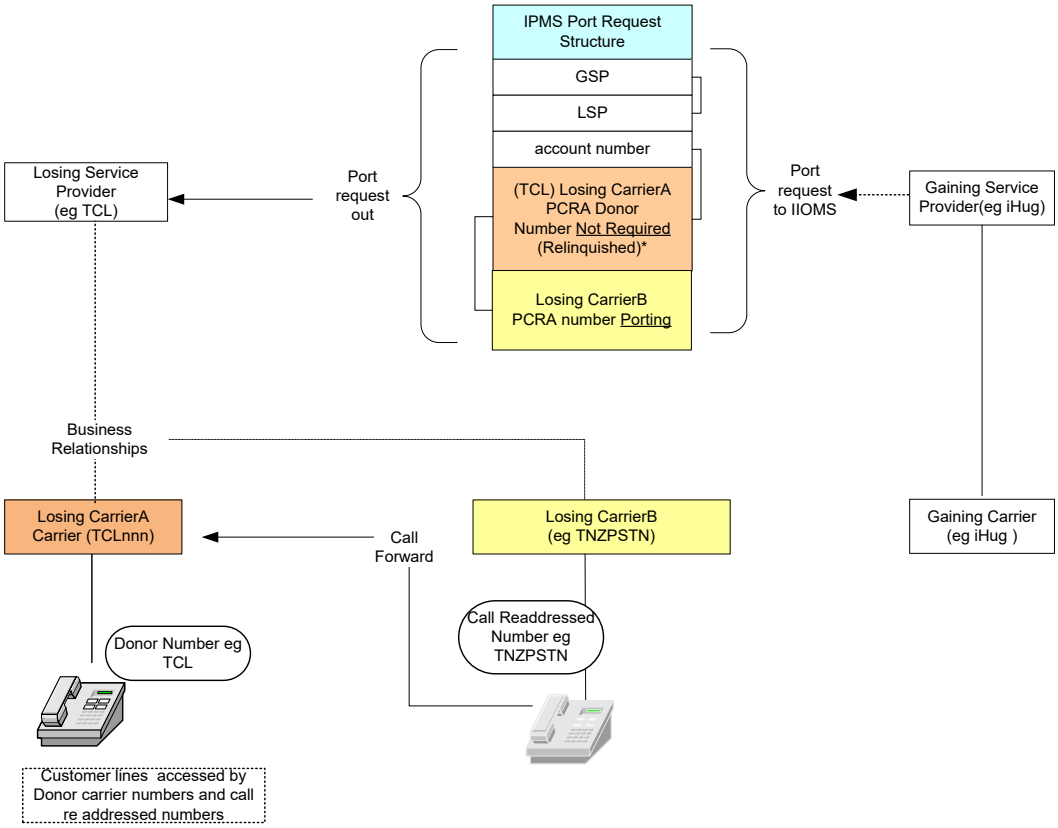
4.1 The following rules MUST then be adhered to by the GSP for the successful approval of Partial Call Readdress numbers to be ported via LMNP process.

- Load port request with correct LSP and Customer a/c number. All Call Readdress associated numbers to be ported must be shown including numbers that may not be required (i.e. both VF and Spark);[3]
- Use checkbox and tick if specific numbers are "not required";
- Submit as per standard rules;
- IPMS will reject giving a reason that a specific number requested is not owned by the LSP specified. When this occurs reconfirm that the LSP is correct and tick the "Override Service Provider" checkbox and resubmit; and
- In "Additional Customer Information" field please add "Call Readdress".

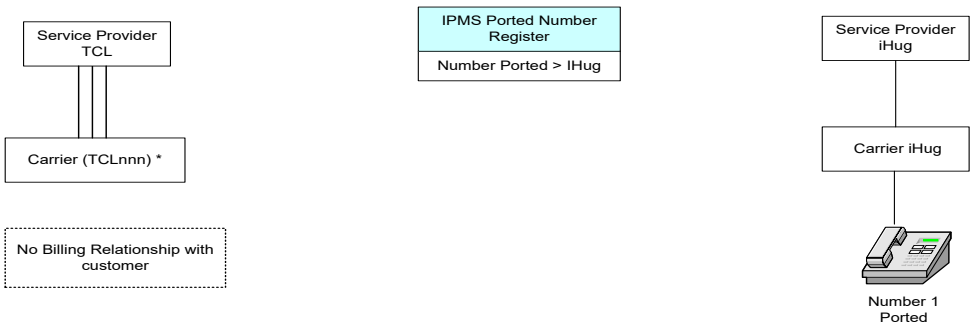
[3] Where Partial Call Readdress numbers are not known by the Customer, the Customer should in the first instance, seek the information from the LSP. The Customer may also authorise the GSP to seek this information on their behalf from the LSP who is to assist in providing it through an agreed escalation process.

Scenario 1

Customer has a call re addressed number and a donor number. They want to port the readdressed number and relinquish the donor number.



Post Port Status

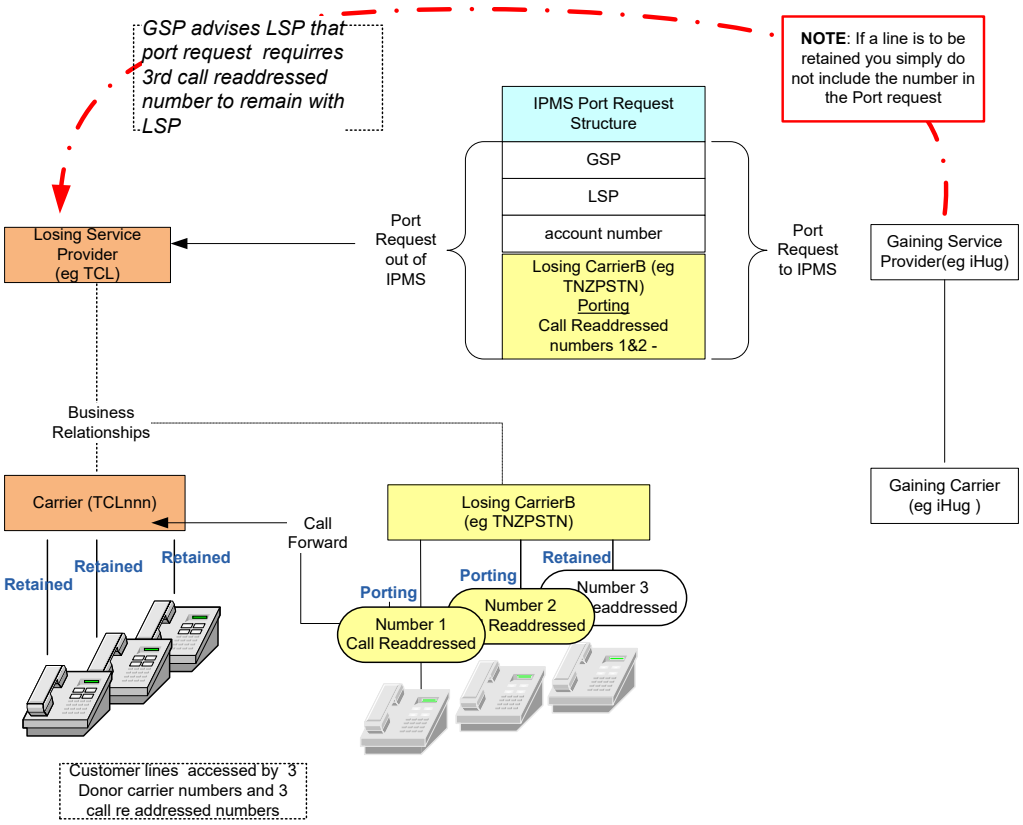


Customer has requested that one number remain with the existing network?

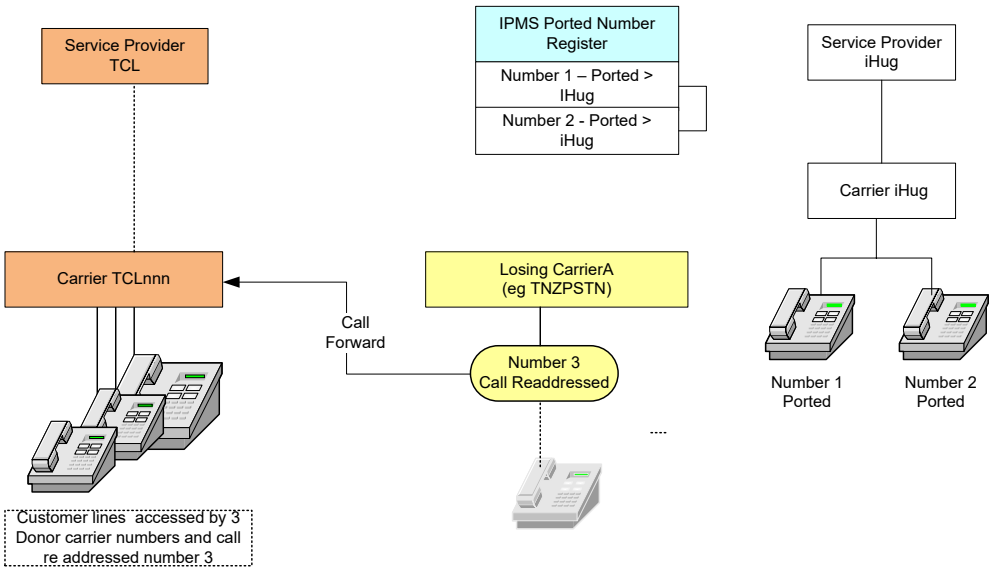
4.2 If Customer requests to remain with both GSP and LSP by splitting the Call Readdress related numbers this must be communicated through standard escalation process before submitting request for validation

Scenario 1

Customer has three Call Readdressed numbers and three donor numbers. They want to port two of the readdressed numbers and retain the three donor numbers and one of the call readdressed numbers.



Post Port Status



Call Readdressed ports involving Resellers

4.3 Where the LSP is a Reseller and the port request includes the porting out of resold Partial Call Readdressed numbers, the wholesaling company is to ensure that business processes are in place whereby the Reseller is able to gain access to the Partial Call Readdress number information.

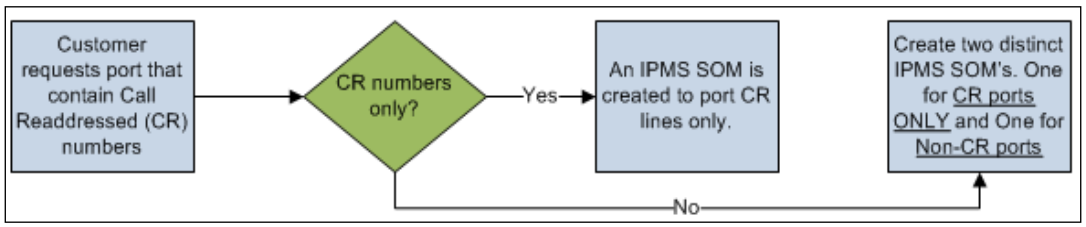
4.4 This is applicable to two scenarios:

- Where the GSP has told the Customer to approach the LSP (Reseller) to gain the necessary Call Readdress information.
- Where the Reseller is both LSP and GSP i.e. change of Carrier, no change of Service Provider for ports involving Call Readdressed numbers.

4.5 Where the LSP is a Reseller, the appropriate IPMS Carrier/Service Provider relationships are to be in place such that Port Request of the call readdressed number is validated by IPMS without the need for invoking the SP Override function in IPMS.

Customer has requested to port numbers that are Call Readdressed and non-Call Readdressed?

4.6 IPMS SOM requests must not contain both Call Readdressed and Non-Call Readdressed lines.



APPENDIX E. ENFORCEMENT AGENCY PROCEDURES

1 The Enforcement Agency

1.1 The Enforcement Agency is a person nominated by the TCF and approved by the Commerce Commission or, where the TCF has failed to nominate a person, a person appointed by the Commerce Commission. The Enforcement Agency is envisaged in clauses 114 to 133 of the Network Terms and clauses 127 to 140 of the LMNP Terms.

1.2 The Enforcement Agency is not a specifically constituted body, but rather will be appointed on an ad hoc basis and will perform its functions in accordance with the powers and processes set out in this part of the Manual.

1.3 The role of the Enforcement Agency under the Network Terms and the LMNP Terms (collectively "the Terms") is to monitor and as required by the Terms measure and enforce compliance with:

- the Equivalent Service provisions in accordance with clauses 112 and 113 of the Network Terms (the Equivalent Service Criteria); and
- the specified service levels set out in clauses 127 to 140 and Table 2 of the LMNP Terms (the LMNP Service Levels).

1.4 Where necessary, the Enforcement Agency will conduct audits of Carriers (Audit Carriers) to assess compliance with the Equivalent Service Criteria and/or the meeting of LMNP Service Levels. For the purposes of APPENDIX E where the context requires, Audit Carrier shall include reference to an Audit Carrier under the Network Terms and an Audit IPMS Client under the LMNP Terms.

1.5 The Enforcement Agency may conduct such audits itself, or appoint an independent expert to conduct the audit on its behalf. Reference to "Enforcement Agency" should be read to include any duly appointed independent expert.

1.6 An expert appointed by the Enforcement Agency is to be independent of both the Audit Carrier and any Carrier whose complaint to the Enforcement Agency initiated the Audit. An expert will be deemed independent of a Carrier if they have not (and no member of their staff involved with the audit have) been retained by that Carrier on any matter within the previous three (3) year period.

1.7 The powers and processes set out here are additional to, and not exclusive of, any other rights a Carrier may have under the Telecommunications Act, at law or in equity.

2 Powers of the Enforcement Agency

Carrier Non Compliance

2.1 Where a Carrier complains in writing to the Enforcement Agency that another Carrier is either not complying with the Equivalent Service Criteria or not meeting the required LMNP Service Levels, the Enforcement Agency may initiate an audit of the Carrier in question. The Enforcement Agency may only commence an audit where a complaint is supported with evidence that, in the view of the Enforcement Agency, establishes reasonable grounds of non-compliance to commence an audit. The Enforcement Agency has the discretion to decline to

conduct an audit if it reasonably considers that the breach complained of is not of a significantly material nature to warrant an audit of the relevant Carrier or if the relevant Carrier satisfies the Enforcement Agency that it has remedied the breach.

2.2 The purpose of undertaking an audit is for the Enforcement Agency to assess and determine whether, as the case may be, the Audit Carrier has:

- complied with the Equivalent Service Criteria; or
- met the LMNP Service Levels; subject to any exemptions granted to the Audit Carrier in respect of the Equivalent Service Criteria or the LMNP Service Levels.

2.3 If, prior to the commencement of an audit an Audit Carrier accepts that it has not complied with the Equivalent Service Criteria or the LMNP Service Levels, the Audit Carrier may request that the Enforcement Agency waive the requirement for an audit and move directly to whatever enforcement action is appropriate under the Terms.

2.4 A Carrier who having been audited is found to comply with the Equivalent Service criteria cannot be subject to another Enforcement Agency audit to assess compliance with the same Equivalent Service Criteria within the six (6) month period following the completion of that audit.

2.5 A Carrier who having been audited is found to comply with the LMNP Service Levels cannot be subject to another Enforcement Agency audit to assess whether it has met the same LMNP Service Levels within the six (6) month period following the completion of that audit.

2.6 Where the Enforcement Agency has commenced or proposes to commence an audit of a Carrier, that Carrier must advise the Enforcement Agency of any exemption granted to it by the Commerce Commission relevant to the commenced or proposed audit.

2.7 Where the Audit Carrier is exempted from complying with some of its obligations either under the Network Terms in respect of the Equivalent Service Criteria or under the LMNP Terms in respect of the LMNP Service Levels and it is those obligations that would be the subject of the audit the Enforcement Agency will suspend any audit or sanction of the Audit Carrier. Any such suspension will be:

- for as long as, and to the extent that, the exemption exempts compliance with the Equivalent Service Criteria or the meeting of LMNP Service Levels; and
- notified to all interested parties by the Enforcement Agency.

2.8 Where requested by the board of the TCF the Enforcement Agency may perform an investigatory and reporting function in respect of the enforcement of Carriers and Service Providers obligations under the IPMS Access Agreement provided to those parties by the TCF.

3 Audit Procedures

Notice Period to any Carrier of Audit

3.1 The Enforcement Agency shall give not less than five (5) Business Days prior written notice to any Carrier of a decision to undertake an audit of the Audit Carrier. The Enforcement Agency shall specify in reasonable detail those aspects of the service and documentation it proposes to audit and will advise the Audit Carrier who is to undertake the audit.

3.2 Any written notice of the Enforcement Agency's intention to conduct an audit must be addressed to the General Counsel / Chief Legal Advisor of the Carrier in question.

3.3 The Audit Carrier shall have five (5) Business Days to agree to the audit, accept the allegation of non-compliance with the LMNP Service Levels or the Equivalent Service Criteria and request that the audit not be undertaken, or submit in writing to the Enforcement Agency why the audit should not be undertaken.

3.4 The Enforcement Agency will consider any submission made in good faith and will then advise the Audit Carrier within five (5) Business Days whether or not an audit will be undertaken. If no submission is received from the Audit Carrier, or the Audit Carrier advises that it agrees to the audit, the Enforcement Agency may, but is not required to, undertake the audit.

3.5 If the Enforcement Agency decides to undertake an audit, then the Enforcement Agency shall:

- provide to the Audit Carrier, not less than five (5) Business Days' notice of the date of the commencement of the audit;
- provide the Audit Carrier a written list of those documents, or such descriptions of the type of documents, it wishes the Audit Carrier to provide to it. Such documents must in the Enforcement Agency's view be necessary to assess whether the Audit Carrier has complied with, as the case may be, the Equivalent Service Criteria or the LMNP Service Levels. Without limitation, this may include documentation pertaining to those documents, records, written practices, data and other documentation within its control that is reasonably necessary to complete an audit; and
- use its reasonable endeavours to conduct the audit in a manner so to provide minimal disruption to the day-to-day business activities of the Audit Carrier.

3.6 Within 10 Business Days of receiving a written request from the Enforcement Agency for documents or such longer period as is reasonably required by the Audit Carrier given the nature and volume of the documents requested, the Audit Carrier must supply the Enforcement Agency with the requested documents within its control and that are reasonably necessary to complete an audit.

3.7 The Audit Carrier will co-operate fully with the Enforcement Agency to facilitate a timely audit process. Such co-operation extends to an Audit Carrier responding to any reasonable written questions from the Enforcement Agency seeking clarification on any of the documents supplied to the Enforcement Agency.

3.8 Where an Audit Carrier fails to supply any requested document(s) it must provide reasons to the Enforcement Agency.

3.9 An Audit Carrier is under no obligation to provide the Enforcement Agency with any documentation for which privilege is claimed or in respect of which the Audit Carrier owes obligations of confidentiality to a third party and that third party does not consent to the disclosure.

3.10 Failure by an Audit Carrier to supply the Enforcement Agency with requested documentation or respond to written questions clarifying such documentation will be deemed to constitute a non-compliant audit, unless such requests and/or questions are not reasonably necessary to

complete an audit. Within 20 Business Days of receiving such requested documents, the Enforcement Agency will provide a copy of the Audit Report to the Audit Carrier setting out its determination (being only a positive or a negative determination) on whether the Audit Carrier has either complied with the Equivalent Service Criteria or met the Service Levels in the LMNP Terms. Such an Audit Report will detail the reasons behind the Enforcement Agency's determination.

3.11 The Enforcement Agency will provide the Audit Carrier five (5) Business Days to comment on any audit report provided to it before a final audit report is issued. The Enforcement Agency will forward a copy of the final audit report to all Carriers who were a party to the Number Portability Determination.

Confidentiality

3.12 All confidential information obtained by the Enforcement Agency in conducting an audit must be kept confidential to the Audit Carrier and the Enforcement Agency.

4 Audit Cost Allocation

Audit Costs

4.1 The Audit Costs associated with completing an Audit Report will comprise of both:

- The Enforcement Agency's reasonable direct costs in respect of the audit (including auditing and legal fees); and
- Such costs of the Audit Carrier in respect of time involved in assisting the audit as submitted by the Audit Carrier to the Enforcement Agency and determined by the Enforcement Agency to be fair and reasonable.

4.2 The Enforcement Agency is responsible for determining and notifying the costs associated with completing an Audit Report ("Audit Costs") within 10 Business Days from when it determines the costs of the Audit Carrier as submitted are fair and reasonable.

4.3 Such Audit Costs as determined by the Enforcement Agency will be payable by:

- the Audit Carrier, where an Audit Report concludes that the Audit Carrier has not complied with the Equivalent Service Criteria set out in the Network Terms or the LMNP Service Levels set out in the LMNP Terms, (whichever were alleged to have been breached) irrespective of whether or not the Audit Report was undertaken due to a request from another Carrier; or
- the Carrier at whose request the Audit Report was completed, where the Audit Report concludes that the Audit Carrier has complied with the Equivalent Service Criteria set out in the Network Terms or the LMNP Service Levels set out in the LMNP Terms (whichever were alleged to have been breached).

4.4 Where an Audit Report was completed otherwise than due to a request of a Carrier, each of the Enforcement Agency and the Audit Carrier will bear their own costs in the event the Audit Report concludes that the Audit Carrier has complied with the Equivalent Service Criteria set out in the Network Terms.

4.5 An Audit Carrier is entitled to be reimbursed its costs by the Enforcement Agency where:

- The Audit Report concludes that it has complied with the Equivalent Service Criteria set out in the Network Terms or the LMNP Service Levels set out in the Terms (whichever were alleged to have been breached);
- The Enforcement Agency has received payment in full of the Audit Costs from the Carrier at whose request the Audit Report was completed; and
- The Enforcement Agency has determined that the costs of the Audit Carrier are fair and reasonable.

4.6 All amounts payable to the Enforcement Agency under this part must be paid in full to the Enforcement Agency within 30 days from when the Service Provider or Carrier (as applicable) is notified of the amount payable. Failure to pay monies due will be treated as a breach of the Terms.

4.7 Any reimbursement due of an Audit Carrier's costs must be received within 30 days from receipt in full of the Audit Costs by the Enforcement Agency.

4.8 Where a payment is due and not received in full by the Enforcement Agency by the due date, the Enforcement Agency is entitled to interest on the amount outstanding on a daily basis at the rate of the current 90-day bank Bill Rate plus 4%.

4.9 The table below sets out the Service Level for given steps in the Porting Processes as detailed in the LMNP Terms. The three columns to the right have been added to clarify which Service Levels are currently measured and/or monitored by the Enforcement Agent and have been included for information purposes only.

Action	Party	Process	Local		Mobile		Measured by IPMS	Monitored by the Enforcement Agent (EA)	Comments
			Simple	Complex	Simple Pre-Pay or Post-Pay	Complex Post-Pay			
Responds to Port Request (PR4 to PR6)	LSP	Port Request	Within eight Working Hours	Within two Business Days	Within 30 Working Minutes	Within two Business Days	Can be although not currently measured	No	Not currently measured in IPMS or monitored by the EA as it is not Customer impacting.
Reviews LSP response and Approves/ Rejects (PR6 to PR8)	GSP	Port Request	Within four Working Hours	Within two Business Days	Within 30 Working Minutes	Within two Business Days	Can be although not currently measured	No	Not currently measured in IPMS or monitored by the EA as it is not Customer impacting.
Port as GSP/GC (PA3 to PA5.2 and PA5.4 to PA7)	GSP	Port Activation	Within four Working Hours	Within four Working Hours	Within one Working Hour	Within four Working Hours	Yes	Yes	Currently measured and enforced as this is Customer impacting.
Port as Losing Carrier (PA5-3 to PA5-4)	Losing Carrier	Port Activation	Within one Working Hour	Within Four Working Hours	Within ten Working Minutes	Within Four Working Hours	Yes	Yes	Currently measured and enforced as this is Customer impacting.
Port as 3rd party and Donor Carrier (PA8 to PA12)	Other Carrier and Donor Carrier	Port Activation	Within one Working Hour except during a planned outage[1]	Within one Working Hour except during a planned outage[1]	Within one Working Hour except during a planned outage[1]	Within one Working Hour except during a planned outage[1]	Yes	Yes	Currently measured and enforced as this is Customer impacting.

Action	Party	Process	Local		Mobile		Measured by IPMS	Monitored by the Enforcement Agent (EA)	Comments
			Simple	Complex	Simple Pre-Pay or Post-Pay	Complex Post-Pay			
APC Response to request (APC3 to APC5)	Responding Party (GSP or LSP)	Approved Port Change	Within two Working Hours	Within four Working Hours	Within two Working Hours	Within four Working Hours	Can be although not currently measured	No	Not currently measured in IPMS or monitored by the EA as it is not Customer impacting.
APC update service orders from APC changes (APC7 and APC8)	Gaining Carrier and Losing Carrier	Approved Port Change	Every Working Hour	Every two Working Hours	Every Working Hour	Every two Working Hours	Can be although not currently measured	No	Not currently measured in IPMS or monitored by the EA as it is not Customer impacting.
Relinquishment of Ported Number (NR2)	Host Carrier	Ported Number Relinquishment	Within five Business Days	Within five Business Days	Within five Business Days	Within five Business Days	No	No	Not able to be measured by IPMS
Relinquishment as 3rd party and Donor Carrier (if required) (NR2 to NR4)	Other Carrier and Donor Carrier	Ported Number Relinquishment	Within one hour except during a planned outage[1]	Within one hour except during a planned outage[1]	Within one hour except during a planned outage[1]	Within one hour except during a planned outage[1]	Can be although not currently measured	No	Not currently measured in IPMS or monitored by the EA as it is not Customer impacting.
Confirmation of service order deletion for Port Expiry (PE5 to PE8)	Gaining Carrier and Losing Carrier	Port Expiry	Within four Working Hours	Within four Working Hours	Within four Working Hours	Within four Working Hours	Can be although not currently measured	No	Not required to be measured in IPMS (stated in LMNP Terms)

Action	Party	Process	Local		Mobile		Measured by IPMS	Monitored by the Enforcement Agent (EA)	Comments
			Simple	Complex	Simple Pre-Pay or Post-Pay	Complex Post-Pay			
Port Withdrawal (entire process)	GSP	Port Withdrawal	Within four Working Hours	Within four Working Hours	Within four Working Hours	Within four Working Hours	Can be although not currently measured	No	Not required to be measured in IPMS (stated in LMNP Terms)
Confirming Port Withdrawal (PW3 to PW5)	Losing Carrier	Port Withdrawal	Within two Working Hours	Within two Working Hours	Within two Working Hours	Within two Working Hours	Can be although not currently measured	No	Not required to be measured in IPMS (stated in LMNP Terms)

[1]To the extent that the planned outage occurs between 8.00 pm and 6.00 am Monday to Sunday, between 4.00 pm and 6.00 am Sunday to Monday and between 4.00 pm on Public Holidays to 6.00 am the following day.

Where the SOM count per Service Provider or Carrier is:

- more than 40 for Mobile Numbers or Local Numbers in a calendar month, Parties are expected to meet these Service Levels 95% of the time.
- 40 or less for Mobile Numbers or Local Numbers in a calendar month, Parties are expected to have no more than 2 failures. The Enforcement Agency will have discretion to investigate cases where a Party regularly fails to meet a Service Level on 2 occasions per calendar month and, in the Enforcement Agency's view it appears to be a systemic issue.

The measurement of the achievement of the Service Levels for Local and Mobile SOMs in each case includes the combined results for Simple and Complex Ports.

APPENDIX F. SECURITY POLICIES FOR IPMS

Since IPMS went live in April 2007, the TCF has granted access to the system to Parties to the Determination and third parties (including Resellers as well as SMS providers, emergency services operators and other Ministries and interested parties).

Security requirements for individual access to IPMS have been left primarily to the companies that execute an IPMS Access Agreement with the TCF, providing that the company itself remains liable for any misuse by their "Authorised Users". There have also existed a number of unwritten policies and procedures to ensure the ongoing security of the IPMS system.

Following the recommendations of the Voco Report dated March 2014, the policies for access to IPMS are set out below.

1 General Policies and Procedures

1.1 Given the critical nature of the IPMS system, the TCF recognises the importance in having oversight of who uses the system and ensuring that Parties to the Determination and other authorised entities that use IPMS adhere to good security practices.

1.2 The following items list the good security practices the TCF requires:

- No user, including the ipmsadmin user can see user passwords; they are obscured in a hashing algorithm. Passwords can and should be changed when required by this policy.
- Individual users should have individual user accounts. The use of admin-class accounts should be limited to managers and key personnel only. There should be a minimum of 2 admin-class accounts per company to ensure redundancy if one account is locked out or the staff member leaves the organisation. Admin-class accounts should not be used for automated systems.
- IPMS does not allow the ipmsadmin account to perform account maintenance on non-admin accounts. It is the responsibility of the admin class account users to maintain their own individual users. Admin-class account users should regularly, at least twice a year, review the needs and requirements of their individual users and ensure that they have the level of access appropriate to their role. Similarly, the ipmsadmin should review the needs of admin-class account users at least twice a year to ensure that all policies and requirements of IPMS are being met (such as password expiry length and the number of admin-class accounts).
- Because the logs and archive requires user accounts to remain in place even when they have become inactive, user accounts can never be deleted. User accounts should be made inactive as soon as practicable after an admin-class account user becomes aware that the individual user no longer requires access to IPMS. The ipmsadmin can and should make accounts inactive if he becomes aware that an individual user has left an organisation or no longer requires access and this has not been done by the admin-class account user within a reasonable time.

- In some cases, the NP Coordinator may have a company specific admin account (RCAdmin) within a Carrier. This is created in all Carriers and is used only for Carrier account administration where there is urgent need.
- Automation (API) accounts may have a long password expiry (9999 days) because it can be expensive and difficult to change passwords in automation, especially if poor design means that the password is stored in multiple locations. The disabling of automation accounts can cause widespread inconvenience to the industry. To minimise the risk of potential breach, API accounts should have long passwords of at least 10 made up of randomised letters, numbers and/or symbols.
- Individual users and admin-class account users should have the passwords changed no less frequently than every 90 days.
- Weekly reports are sent to the NP Coordinator on expired and expiring passwords. The NP Coordinator will review and note these. If an API account is involved, the NP Coordinator should take immediate action along with the Carrier to reset this password. If individual admin accounts are noted, the NP Coordinator is to log these and raise them with the Carrier if they appear in the following week's list of expired passwords.
- Error logs are sent to the NP Coordinator weekly, these are logged and graphed. Any spikes or trends are closely examined and relevant Carriers are contacted about their processes, and asked to explain. Advice can be given on possible solutions and improvements.
- API activity is logged daily, tabled and graphed weekly, and reviewed by the NP Coordinator. Spikes or unusual activity are investigated and followed up with Application Support or the Carrier concerned.

2 Escalation

2.1 Any highly abnormal activity or activity which would indicate that a user's account has been compromised or used contrary to this security policy should be raised by the NP Coordinator with the Carrier concerned and the Forum Administrator immediately. Any such activity must be investigated thoroughly to rule out any instance of a malicious use of IPMS. The account may be made inactive during this time to rule out third party involvement.

2.2 The Forum Administrator and the NP Coordinator will inform the TCF CEO of the relevant event and the work in progress to identify or resolve the event as soon as practicable. The TCF CEO will be responsible for informing the TCF Board of the matter in due course.

APPENDIX G. BILATERAL AGREEMENT CHECK LIST

The purpose of this section is to provide an indicative list of the items which, eventually, would need to be discussed and approved in the Bilateral Agreement between two Service Providers who are parties to the LMNP Terms.

LMNP BILATERAL DISCUSSION KICK-OFF QUESTIONNAIRE

OVERVIEW

> *"In a Number portability environment changes are required to the traditional way in which calls are routed from originating Carriers to terminating Carriers. For voice services, this applies to local, national, fixed-to-mobile, mobile-to-fixed, mobile-to-mobile, incoming and outgoing international and other calls involving local or mobile numbers."*
>
> ……..……Pg 4 of Network Terms for Local & Mobile Number Portability in New Zealand [29.08.2005]

This document is intended to be used by New Zealand telecommunications network operators to initiate bilateral technical negotiations with other network operators aimed at facilitating agreement about the call handling interworking arrangements to be used in the Local and Mobile Number Portability (LMNP) environment.

Interworking arrangements between networks will need to specify which of the several options allowed for in the Network Terms will be implemented by network operators for handling calls passed across the boundaries between their networks when Number Portability is operational. Specifically, each network that originates calls, or transits toll bypass calls, must either:

- Perform a call-by-call lookup of a Number Portability database to determine whether a called number is Ported, and if it is Ported, determine the Recipient Network (identified by the 011xn7 Handoff Code (HOC) that now hosts the number, and then route the call towards that network by appending the HOC to the Called Party Number,

OR

- Pass the call to another network which is delegated to perform all or part of the above function on its behalf. In this case there are further options allowed by the Network Terms that must be selected. These cover the format of the Called Party Number signalled with the call, and whether the call is to be onward-routed by the delegated network, or released for Query on Release (QOR) action or for Redirection action by the originating (or transit) delegating network.

In addition, network operators need to confirm other aspects of LMNP call handling such as default call routing under abnormal circumstances such as database failure, and methods of protecting the network against call recirculation.

USING THE TEMPLATE

This template is designed as a tool to help network operators implement LMNP. It has been drafted as a guideline only and is not compulsory.

The information collected from this questionnaire will be treated as confidential between the parties and will not be disclosed to any other party, unless such disclosure:

- is agreed to by the parties; or
- is required by law.

The information is intended to be used as an input to bilateral negotiations to determine the necessary changes to call handling functionality required to implement LMNP. The agreed network arrangements will then be documented and included in a revised interconnection agreement between the network operators.

Terminology used in this document is in accordance with the reports "LMNP Terms" and "Network Terms" dated 2.12.2021.

NOTES ABOUT THE QUESTIONNAIRE

Q1 – Q4: relate primarily to your network acting as a Recipient Network hosting numbers Ported from other networks, and will only be applicable if you provide a (terminating and originating) local service to Customers. The information will enable other networks to set up call routing data required to deliver calls to numbers Ported into your network.

Q2: Actual allocation of HOCs is done via the Number Administration Deed (NAD – www.nad.org.nz). Most Carriers are expected to have a single 011xnt (t=7, 8, or 9) value assigned, however some are proposing to use multiple codes where they support two or more distinct networks. Separate HOCs are expected for fixed and mobile applications operated by the same Carrier.

Q3 & Q4: This information will assist with confirming that call recirculation cannot occur in abnormal situations.

Q5 & Q6: indicate whether your network will consult a Number Portability database itself to determine call routing [case (a)], or will delegate this function to another network by routing calls to that network without first consulting a database [case (c)].

Case (b) is a mixed case where your network checks some number ranges, and delegates checking other number ranges to another network. For cases (b) and (c) this information in conjunction with Q7 will enable other network operators to offer to act as a delegated network to consult their Number Portability databases on your behalf.

Note that only Customers' local (fixed network) and mobile numbers are able to be Ported under LMNP. Therefore no changes are required to the routing of calls to numbers delivered on the interconnect boundary in other formats (e.g. 0800, 0900, 010, 111 etc.).

Q7 & Q8: This information will enable the network(s) with which you are directly interconnected to set up call routing data to transit to the relevant Recipient Networks calls destined to Ported (and non-Ported) numbers that have been received from your network. NOTE that the descriptions 0a(2-8) and 0A9 are typical of the ranges described, but not exhaustive.

Q9: covers the details of call handling in the situation where you intend to delegate Number Portability database consultation to another network. It will need to be completed as an iterative process in conjunction with the delegated network; therefore it may not be possible to complete some parts of Q8 on the initial pass.

Note that the delegated network [identified in Q9(c)] does not necessarily need to be directly interconnected with your network. By using the 011xn8 and 011xn9 HOCs to identify the delegated

network, calls can be routed via a transit network [identified in Q9(a)] (which will not consult the database) to the specified delegated network (which will). Where the delegated network is directly connected to your network the use of a HOC is optional if the default action is for the delegated network to consult the database for all incoming calls on a given incoming route (as will be the case for international incoming calls, for example, because they will never include a HOC). In this situation there is no need to change the existing called party number format passed between the delegating and delegated networks.

9(d) is used to identify which of three call routing mechanisms allowed for by the LMNP Terms (Onward Routing, Query on Release [QOR] or Redirection) you wish to operate in conjunction with the delegated network. If QOR or Redirection are to be used there will need to be further detailed technical discussions as these functions are not supported in the PTC331 No.7 Signalling standard currently used for network interconnection in New Zealand.

Q10: This information will assist with confirming that recirculation cannot occur in abnormal situations.

Q11 & Q12: This information will advise other networks whether your network can act as a delegated network and consult a Number Portability database on another network's behalf, and if so, the specific method(s) of call routing available.

Q13 & Q14: This information can be used to progress the resolution of issues concerning geographic-origin based routing in the LMNP environment.

Carrier Name	
Contact Person	
Contact email address/telephone	
Date questionnaire completed	

Q	QUESTION	ANSWER (please ☒ as appropriate)	
1	*Will your network act as a Recipient Network for Ported numbers (i.e. will you be, or host, one or more Gaining Service Providers)?*	(a) NO – go to Q4	☐
		(b) YES – go to Q2	☐
2	*What **011xn7** Hand-off Code(s) (HOC) will your network accept as a prefix to the called party's national number with incoming calls to Ported Customers hosted on your network?*	HOC	Comment

Q	QUESTION	ANSWER (please ☒ as appropriate)	
	Please insert HOC values and description if more than one HOC is used *NOTE: The 011XN7 HOCs are allocated by the NAD*		
		- go to Q3	
3	*What action will your network take if it receives a call from another network with **the called party number prefixed with one of your 011xn7 HOCs** (from Q2), but cannot terminate the call because the number range is not installed or the number is not allocated to a Customer on your network?* (i.e. other network's database is not up-to-date) **NB** the Cause Value in question 3(a) is the Cause Value sent over the interconnect boundary.	(a) always release the call (Cause Value =)	☐
		(b) other (please describe)	☐
		NOTE: To prevent any possibility of recirculation your network must NOT change or delete the received HOC and onward-route the call! *- go to Q4*	
4	*What action will your network take if it receives a call from another network with **the called party number in the format 0+NN**, where NN is a number range allocated to your network, but cannot terminate the call because the number is not allocated to a Customer on your network?* *NN= National Number* **NB** the Cause Values in question 4(a) and (b) are the Cause Values sent over the interconnect boundary.	(a) always release the call (Cause Value =)	☐
		(b) determine if the number has Ported to another network & if so, attach 011xn7 HOC and onward route the call. Otherwise release the call (Cause Value =)	☐
		(c) other (please describe)	☐
		- go to Q5	
5	*For calls to NZ local network Customers' numbers*	(a) YES – for ALL called local network numbers	☐

Q	QUESTION	ANSWER (please ☒ as appropriate)		
	originated by Customers (if any) on your network, and/or *transited by your toll bypass network (if any)* ***will your network check a Number Portability database** to determine the Ported status of the called number, and, if Ported, determine the HOC identifying the Recipient Network (before routing the call to another network)?*	(b) YES – for some called local network numbers		☐
		(c) NO		☐
		- go to Q6		
6	*For calls to NZ mobile network Customers' numbers* *originated by local Customers (if any) on your network, and/or* *transited by your toll bypass network (if any)* ***will your network check a Number Portability database** to determine the Ported status of the called number and, if Ported, determine the HOC identifying the Recipient Network (before routing the call to another network)?*	(a) YES – for ALL called mobile network numbers		☐
		(b) YES – for some called mobile network numbers		☐
		(c) NO		☐
		- go to Q7		
7	*For which Customers' number ranges will your network **consult a Number Portability database** to determine porting status and, where Ported, determine the HOC identifying the Recipient Network?* *(A=area code digits 3,4,6,7,9)* *(Please split the number ranges if required to differentiate)*	Not applicable as Q5(c) and Q6(c) both apply. - *go to Q9*		☐
		021	One NZ mobile range	☐
		027	Spark mobile range	☐
		029	One NZ mobile range	☐
		02x	Other mobile ranges	☐
		0A(2-8)	Local ranges	☐
			Your network's own ranges	
		0A9	Other non-Spark local (fixed line) ranges	

<table>
<tr><th>Q</th><th>QUESTION</th><th colspan="4">ANSWER (please ☒ as appropriate)</th></tr>
<tr><td></td><td></td><td></td><td>Other network's number ranges as appropriate</td><td></td></tr>
<tr><td></td><td></td><td></td><td>Other network's number ranges as appropriate</td><td></td></tr>
<tr><td></td><td></td><td colspan="2">- go to Q8</td><td></td></tr>
<tr><td>8</td><td colspan="4">To which network(s) will you deliver calls to NZ local and mobile network Customers' number ranges whose porting status has been determined by your network and found to be either (i) Ported to Recipient Networks identified by 011xn7 HOCs as follows; or (ii) not ported?</td><td></td></tr>
<tr><td></td><td>Recipient Network</td><td>HOC</td><td>Calls will be routed on <u>direct</u> routes to the following Network:</td><td>Calls will be routed on <u>alternate/overflow</u> routes to the following Network:</td><td></td></tr>
<tr><td></td><td>For example
Big Bird Networks</td><td>011747</td><td>Internally Routed</td><td>Not applicable</td><td></td></tr>
<tr><td></td><td>For example
Spark</td><td>011647</td><td>Spark</td><td>No overflow routing via other networks</td><td></td></tr>
<tr><td></td><td>See Carrier tab of Config Worksheet for details</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="4">……. - go to Q9</td><td></td></tr>
<tr><td>9</td><td colspan="4">How & where will you deliver calls to those NZ fixed and mobile network Customers' number ranges whose porting status is NOT checked by your network?</td><td></td></tr>
<tr><td></td><td colspan="3">Not applicable as Q5(a) and Q6(a) both apply. - go to Q10</td><td>☐</td></tr>
<tr><td></td><td>(a) Calls will be routed on direct routes to the following Network(s)……..:</td><td colspan="2">(please specify network.
NB this network will be referred to as Network x in Q 9[c])</td><td></td></tr>
<tr><td></td><td rowspan="4">(b)…. with the called party number parameter sent on the direct route in the following format:</td><td>either:</td><td>0+NN</td><td>☐</td></tr>
<tr><td>or:</td><td>011xn8+NN (xn=)</td><td>☐</td></tr>
<tr><td>or:</td><td>011xn9+NN (xn=)</td><td>☐</td></tr>
<tr><td colspan="3">(please specify xn value if used)</td></tr>
</table>

Q	QUESTION	ANSWER (please ☒ as appropriate)			
		(c) Database lookup will be performed by the following Network(s) delegated to do this on your behalf	(*if 0+NN format is used in 9[b], then this network must be the same as Network x*)		
		(d) What action do you want the delegated network to take if it determines that a number is Ported?	either:	attach 011xn7 HOC to called party number and onward route	☐
			or:	release call with Cause Value 14 (for QOR treatment in your network)	☐
			or:	release call with Cause Value 23 & Redirecting Number (for Redirection treatment in your network)	☐
		- go to Q10			
10	*What action will your network take if it attempts to consult a Number Portability database to determine the Ported status of a called number, but finds that the **database is unavailable**?*	Not applicable as Q5(c) and Q6(c) both apply. *- go to Q13*			☐
		(a) always release the call			☐
		(b) route the call based on the called number (i.e. assume that the called number is not Ported)			☐
		(c) other (*please describe*)			☐
		– go to Q11			
11	*Is your network able to act as a delegated network and consult a Number Portability database on behalf of other networks?*	(a) NO *– go to Q13*			☐
		(b) YES *– go to Q12*			☐
12	*Which method(s) of call handling does your network offer when acting as a delegated network, when a called number is found to be Ported?*	(a) will attach 011xn7 HOC to called party number and onward route			☐
		(b) will release call with Cause Value 14 (for QOR treatment in the delegating network)			☐

Q	QUESTION	ANSWER (please ☒ as appropriate)	
		(c) will release call with Cause Value 23 & Redirecting Number (for Redirection treatment in the delegating network)	☐
		– go to Q13	
13	*Is your network able to support the sending of the ITU-T ISUP Location Number parameter with calls made by Ported numbers hosted on your network (to identify the geographic location of the Customer to other networks receiving the calls?*	(a) Not Applicable (as Q1(a) applies)	☐
		(b) NO	☐
		(c) YES	☐
		– go to Q14	
14	*Is your network able to receive the ITU-T ISUP Location Number parameter with incoming calls from other networks and use the information contained in the parameter in geographic-origin based call routing (e.g. typically for 0800/0808 & 0900 calls)?*	(a) Not Applicable (as geographic-origin based routing is not used)	☐
		(b) NO	☐
		(c) YES	☐
15	Other Comments:		
	end of questionnaire		

APPENDIX H. IPMS MANAGEMENT

This section, and the definitions it contains, relate exclusively to the IPMS.

"**Fault**" means the failure, in whole or in part, in the supply of, or a material degradation in the quality of, the IPMS or a failure to provide any data, report or document to TCF or Service Providers or Carriers as required by the IPMS Agreement and the Number Portability Determination;

"**Fault Severity**" means the level of severity of any Fault, as determined by TCF, in accordance with the following:

Severity	Definition
Critical	• IPMS is unavailable to TCF or Service Providers or Carriers; or • Severe operational impact degrading the performance or outputs of the IPMS; or • The IPMS (or any output from the IPMS including TCF Data) is affecting the integrity or correct operation of any telecommunications network used by any Service Providers or Carriers.
High	Significant operational impact affecting portions of the IPMS or impacts on the ability of the IPMS to perform effectively.
Medium	Allows the IPMS to continue to operate (possibly with a work-around in place (at no additional cost to TCF, unless agreed otherwise with TCF in writing)) but a minor part of it is unavailable or not working as contemplated under this Agreement.
Low	Non-critical to TCF or Service Providers or Carriers.

"Help Desk" means System Administrators Help Desk which is contacted by telephone or email as set out in section 5 of APPENDIX H, or such alternative phone number or email address as the TCF may, from time to time, advise Service Providers or Carriers in writing;

"**IPMS Planned Outage**" means the temporary unavailability of the IPMS in order for the System Administrators to carry out any testing, repair or maintenance which is reasonably required in respect of the IPMS;

"Performance Levels" means the performance criteria to which the System Administrator will provide the management services as described in section 4 of APPENDIX H;

"Resolution Time" means the period from the time a Fault is discovered by the System Administrator or is logged by the TCF or a Service Provider or Carrier (in accordance with this Manual) (whichever is the earlier) until the time that Fault has been Resolved (inclusive);

"**Resolved**" means that a Fault has been rectified and the IPMS has been returned to normal operating conditions as reasonably determined by TCF or a Service Provider or Carrier (and "**Resolution**" shall have a corresponding meaning);

"**Response Time**" means the period from the time a Fault is discovered by the System Administrator or is logged by TCF or a Service Provider or Carrier (in accordance with this Manual) (whichever is the

earlier) until the time the System Administrator has advised TCF and Service Providers and Carriers that it has commenced action to diagnose and rectify the Fault (inclusive);

"**System** Administrator" means the party appointed by the TCF from time to time to maintain and operate the IPMS.

"**TCF Coordinator**" means the person appointed by TCF and notified to the Service Providers and Carriers from time to time to liaise with the System Administrator and/or Service Providers and Carriers on matters relating to the IPMS;

"**TCF Data**" means data owned or supplied by TCF or a Service Provider or Carrier to which the System Administrator is supplied access and data which may be generated, compiled, arranged or developed in providing the IPMS;

"**TCF Facilitator**" means the person appointed by TCF and notified to Service Providers and Carriers from time to time to liaise with the System Administrator and/or Service Providers and Carriers on matters relating to the IPMS for escalation purposes.

1 Support Services

1.1 The following support services shall be available:

- The TCF will procure that the System Administrator shall make available the Help Desk to the Service Providers and Carriers on a 24-hour 7 day per week basis, for the purpose of reporting and resolving Faults and operational issues or enquires that arise in relation to the IPMS. The TCF shall notify Service Providers and Carriers in writing of any changes that occur to the relevant telephone or email address of the Help Desk set out in section 5 of APPENDIX H.

1.2 The Help Desk will maintain:

- a reception point for logging Faults and enquires;
- Fault progress tracking and reporting;
- IPMS outage tracking;
- for the duration of any Fault, direct contact, as reasonably required by the relevant Service Provider or Carrier, between the System Administrator and that Service Providers or Carrier's specialist operations groups; and
- a coordination point for the restoration of the IPMS.

1.3 The TCF shall procure that the System Administrator shall, through the Help Desk and after becoming aware of any Fault in respect of Service Providers and Carriers:

- take all action reasonably necessary in order to rectify that Fault, with as little disruption to Service Providers and Carriers as is reasonably possible and in any event in accordance with the Performance Levels;
- advise the TCF Coordinator and the relevant Service Providers and Carriers of any actions being taken in order to rectify the Fault;

- provide the TCF Coordinator and the relevant Service Providers and Carriers with an estimate of the time required to rectify the Fault;
- provide the TCF Coordinator and the relevant Service Providers and Carriers with ongoing progress reports in respect of the actions being taken to rectify the Fault in accordance with the times for the relevant update frequency specified in the Performance Levels as set out in section 4 of APPENDIX H.

1.4 The Service Providers and Carriers shall be responsible for managing its own staff training in relation to the use of the IPMS and shall not call the Helpdesk for this unless agreed otherwise with the TCF Coordinator.

1.5 A breach of the Performance Levels specified in section 4 of APPENDIX H shall exclude any breach which arises:

- due to an event of force majeure; or
- due to a material default by the Service Providers and Carriers of any of its obligations under its Agreement with the TCF; or
- due to a material default by the TCF of any of its obligations under the agreement with the System Administrator or any other support provider other than the obligation to make payment to those parties; or
- due to any material default under any IPMS Access Agreement with the Service Provider or Carrier or between the TCF and any other Service Provider or Carrier; or
- from any act or omission by the Service Provider or Carrier, their officers, employees, agents, Contractors or consultants or any other person for whom the Service Provider and Carrier is responsible other than any act or omission taken or not taken (as the case may be) at the direction of the TCF, its officers, employees, agents, Contractors, sub-Contractors; or
- as a direct result of the malfunction of a Service Provider or Carrier connection or equipment or any other connection or equipment which is not under the control of the TCF; or
- during any Planned Outage.

2 Faults

2.1 Nothing in this Agreement shall require the TCF to provide continuous or fault free access to the IPMS.

2.2 The Service Providers and Carriers shall comply with such specific procedures and obligations in relation to the management of Faults as reasonably required by the TCF.

2.3 The TCF shall procure that the System Administrator shall monitor the IPMS on a 24 hour per day / 7 day per week basis for the purpose of early identification of any Faults, or any circumstances that might reasonably give rise to a Fault.

2.4 On becoming aware of any Fault, Service Providers and Carriers agree that they shall check that the Fault relates to the IPMS prior to notifying the Help Desk. If, after such checking, the Service

Provider or Carrier still believes (acting reasonably) that the Fault is with the IPMS System, the Service Providers or Carrier shall notify the Help Desk by phone (at any time) or by email (only recommended during Working Hours) as soon as reasonably practicable. Each such notice shall specify:

- details of the nature of the Fault; and
- the Fault Severity of that Fault.

3 Response Time

3.1 Upon becoming aware of any Fault in the IPMS, the TCF shall ensure the System Administrator shall comply with the Response Times and Resolution Times in relation to rectification of that Fault and will use its best endeavours to respond to all Faults within a shorter timeframe.

3.2 Only Faults with Critical or High Fault Severity Level will require a Response outside of Working Hours unless otherwise approved by the TCF Coordinator or the TCF.

3.3 The TCF shall procure that the System Administrator will provide an incident report to the Service Providers and Carriers affected by the incident, within 1 Business Day of Resolving a Fault, for all Faults with a Critical or High Fault Severity Level plus any other logged Faults specifically requested.

IPMS Planned Outages

3.4 Subject to sections 3.6 and 3.7 APPENDIX H, the TCF shall use its best endeavours to ensure that all IPMS Planned Outages occur between 12.00am and 04:00am on the first Sunday of each month, and that the IPMS Planned Outage does not exceed these hours.

3.5 Subject to sections 3.6, 3.7 and 3.8 of APPENDIX H, the TCF shall procure that the System Administrator shall give the Service Providers and Carriers and the TCF Coordinator a minimum of 2 Business Days prior written notice of any IPMS Planned Outage. Each such notice shall include the following information:

- the reason for the IPMS Planned Outage;
- the proposed date and time of the IPMS Planned Outage;
- the estimated duration of the IPMS Planned Outage; and
- the name and contact details of the appropriate person whom the Service Providers and Carriers should contact for further information in relation to the IPMS Planned Outage.

3.6 Where the proposed date and time for the IPMS Planned Outage is outside of the timeframe specified in section 3.4 of APPENDIX H and is:

- outside Working Hours, the notice period referred to in section 3.5 of APPENDIX H for the IPMS Planned Outage shall be a minimum of 1 Business Day; or
- within Working Hours, the notice period referred to in section 3.5 of APPENDIX H for the IPMS Planned Outage shall be a minimum of 10 Business Days,

  and in either case, the notice to the Service Providers and Carriers shall include the information referred to in section 3.5 of APPENDIX H and the reason why the IPMS Planned Outage is occurring at that time.

3.7 If the TCF considers (acting reasonably) that any IPMS Planned Outage requires the Service Providers and Carriers to:

- undertake staff training; or
- assist with the IPMS Planned Outage,

then if the date and time of the IPMS Planned Outage is within the timeframe specified in section 3.4, the TCF shall, subject to section 3.8 of APPENDIX H, procure that the System Administrator gives the Service Providers and Carriers a minimum of 10 Business Days' notice or a shorter notice period if agreed by all Service Providers and Carriers.

3.8 Where:

- the IPMS Planned Outage is as a result of a major enhancement to the IPMS (as reasonably determined by the TCF), then the TCF will endeavour to consult with each Service Provider and Carrier prior to the System Administrator giving notice to agree the length of the notice period, and the TCF shall procure, notwithstanding section 3.7 of APPENDIX H, that the notice period shall be a minimum of 20 Business Days or such longer period as agreed to by the TCF;
- the circumstances giving rise to a IPMS Planned Outage are such that an immediate, temporary suspension or restriction of the IPMS is required and the System Administrator is not able to give notice as set out above, the TCF shall procure that the System Administrator shall use its best endeavours to provide the TCF Coordinator and the Service Providers and Carriers with such prior notice as is reasonably possible in the circumstances.

4 IPMS Performance Levels

4.1 The TCF shall endeavour to meet the following Performance Levels:

- Subject to section 1.5 of APPENDIX H, the TCF shall use reasonable endeavours to ensure the IPMS is available 99% (at all times) per quarter.

4.2 The maximum Response Times and Resolution Times are:

Fault Severity	Response Time	Resolution Time	Update Frequency
Critical	30 minutes	4 hours	Every 45 minutes
High	1 hour	8 hours	Every 2 hours
Medium	10 hours (1 day)	50 hours (5 days)	Every second day
Low	20 hours (2 days)	100 hours (10 days)	Every week

4.3 For Faults with a Critical Fault Severity Level, the Response and Resolution Times are based on elapsed hours, all other Fault Response and Resolution Times are based on Working Hours.

4.4 Critical and High Fault Severity Response Times and Resolution Times will only be applied to the production environment. The test and training environment is expected to have a lower priority under normal circumstances.

5 IPMS Monitoring

5.1 The TCF shall procure the continual proactive (24 hours per day 7 days per week) monitoring of the IPMS to enable early notification of failures Faults or issues.

Escalation

5.2 If a Fault is unable to be resolved by the System Administrator within a reasonable timeframe then the relevant Service Provider or Carrier may escalate the problem in accordance with the timeframes identified in the Performance Levels to the System Administrator personnel identified in the Table below.

The Service Provider and Carrier /the TCF Interface

5.3 Each Service Provider and Carrier, by written notice to the TCF and the TCF Coordinator, shall appoint a user administrator ("User Administrator") and shall maintain the appointment of a User Administrator throughout the term of this Agreement. The relevant Service Provider and Carrier may replace, from time to time, by written notice to the TCF and the TCF Coordinator, their User Administrator.

5.4 The principal function of the User Administrator shall be to manage the relationship between the relevant Service Provider and Carrier and the TCF Coordinator and the relationship between the relevant Service Provider and Carrier and the System Administrator, in each case, in accordance with this Manual.

IPMS Escalation Roles and Responsibilities

5.5 Level 1 Contact Points:

System Administrator Help Desk

Responsibility: Management of Call Centre, initial logging of events and escalation of issues.

Contact Details: NP Coordinator and TCF Forum Administrator

5.6 TCF member contacts

Responsibility: Assistance to System Administrator, Future sourcing as required, and liaison with users.

Escalation/ Level	Role	Responsibility	Contact Details
TCF			
Level 2	TCF Coordinator	Escalation of issues	NP Coordinator. Rob Clarke Rob.clarke@tcf.org.nz 021 956 501
Level 3	TCF Facilitator	Escalation of issues not able to be resolved with TCF Coordinator	TCF Forum Administrator. Refer www.tcf.org.nz for contact details.
Parties to the NP Determination			
Representative of each Party to the Number Portability Determination	User Administrators		Contact list is available on the NPUG Shared Drive.

5.7 The TCF may add, amend, delete information in section 5.5 and 5.6 of APPENDIX H, from time to time by notice in writing to the Service Providers and Carriers.

6 Managing the Load on IPMS

6.1 The performance of IPMS is impacted primarily by the following factors:

- the polling frequency of API calls;
- the number of Carriers;
- the number of outstanding ports of a given status;
- the amount of time that SOMs spend in-progress; and
- the number of SOMs being processed per month.

6.2 As IPMS is solely a reactive system, it cannot control the load and is completely dictated to by the users of the system. The following frequencies were agreed by NPUG in the interests of keeping IPMS running smoothly.

Recommended API Polling Frequency (from section 4.5 of the IPMS Technical Specification)

Operation	Conditions	Max Frequency
getRequestedPorts	Filter My SP Action + Date	5 mins for mobile Service Providers 10 mins for local Service Providers
getApprovedPorts	Filter My Carrier Action + statusList + Date	May be called once for each possible Status in the statusList filter within the following periods: 2 mins for mobile Service Providers 10 mins for local Service Providers
getPortProgress	SOM	Once every 5 minutes for each port during activation
getNetworkUpdates	CarrierIdList filter set to null	Once every 10 mins. Set CarrierIdList filter to null to return network updates for all Carriers associated with the user/company.
getApprovedPortChangeRequests	My SP Action	15 mins

6.3 APIs called by automated processes can inflict considerable load on the system. Where a Carrier's system is doing more than what is considered safe, they may be asked to reduce the load. Basic methods to do this include:

- slowing down the frequency of calls;
- reducing the frequency of polling for given events after a certain amount of time (e.g. reduce frequency of getPortProgress after half an hour for a given port and again after four hours); and
- escalating repeated failures (especially security failures, such as 620, PASSWORD_EXPIRED).